Gateway for supporting communications between network devices of different private networks

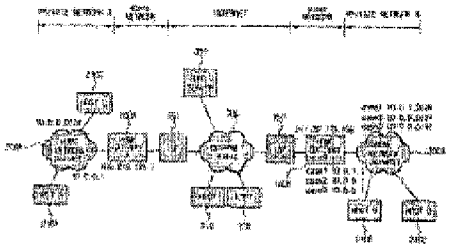
Publication number: CN1525711 (A)
Publication date: 2004-09-01
Inventor(s): JUN-HYEONG KIM [KR]
Applicant(s): SAMSUNG ELECTRONICS CO LTD [KR]
Classification:
- international: ***H04L12/46; H04L29/12;*** **H04L12/46; H04L29/12;** (IPC1-7): H04L12/66
- European: H04L29/12A4; H04L12/46E; H04L12/46V; H04L29/12A
Application number: CN20041007314 20040121
Priority number(s): KR20040001570 20040109; KR20030004126 20030121

Also published as:
CN1301611 (C)
EP1441483 (A2)
US2004218611 (A1)
JP2004229299 (A)

Abstract not available for CN 1525711 (A)
Abstract of corresponding document: **EP 1441483 (A2)**

Disclosed is a gateway under Home-to-Home Tunnelling Initiation Protocol (HTIP), for supporting communications between network devices connected to different private networks. When a tunnel setup request message is received from a host being connected to a first private network to a second private network being connected to a public network, a HTIP processor belonging to a control unit of the gateway communicates with the gateway of the second private network, negotiates necessary information, and sets up a VPN tunnel utilizing the information. If the private networks have identical network address, or if network address of one private network is included in the network address of the other, a new network address table is created such that the two private networks can use different network addresses in the VPN tunnel.; With respect to data packets being transmitted from the host of the first private network, or from the second private network, address is translated based on the new network address table, and therefore, the translated address is forwarded. Because a user in home network can utilize a larger coverage of network, he/she can actively participate through a variety of communities. Additionally, a shortage of IPv4 type public IP addresses under is solved.

FIG 1



[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/66

[12] 发明专利申请公开说明书

[21] 申请号 200410007314.0

[43] 公开日 2004 年 9 月 1 日

[11] 公开号 CN 1525711A

[22] 申请日 2004.1.21
[21] 申请号 200410007314.0
[30] 优先权
[32] 2003. 1.21 [33] KR [31] 4126/2003
[32] 2004. 1. 9 [33] KR [31] 1570/2004
[71] 申请人 三星电子株式会社
地址 韩国京畿道
[72] 发明人 金俊亨

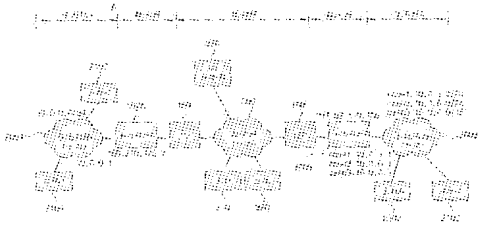
[74] 专利代理机构 北京市柳沈律师事务所
代理人 马 莹 邵亚丽

权利要求书 4 页 说明书 29 页 附图 13 页

[54] 发明名称 用于在不同的专用网的网络设备之间支持通信的网关

[57] 摘要

公开了一种根据本地对本地隧道启动协议(HTIP)，用于支持在连接到不同专用网的网络设备之间通信的网关。当从连接到第一专用网的主机接收到对连接到公共网络的第二专用网的隧道建立请求消息时，属于网关的控制单元的 HTIP 处理器与第二专用网的网关通信，协商必需的信息以建立 VPN 隧道。如果专用网具有相同的网络地址，或专用网的网络地址被包括在另一个的网络地址中，则生成新的网络地址表，使在 VPN 隧道中这两个专用网使用不同的网络地址。数据分组基于新的网络地址表来变换地址，从而转送该变换的地址。在本地网络中的用户可以利用更大范围的网络，可以经由各种各样的社区积极地参与。还解决了 IPv4 类型的公共 IP 地址短缺的问题。



ISSN1008-4274

1.一个网关，包括:

至少一个或多个连接到一个公共网络的公共网络接口;

至少一个或多个连接到一个专用网的本地网接口；和

一个控制单元，用于如果一个隧道建立请求从第一专用网被接收，以建立一个到连接到所述公共网络的第二专用网的隧道，则通过与所述第二专用网的网关通信来建立一个 VPN 隧道，其中，

如果所述第二专用网和所述第一专用网具有同样的网络地址，或者如果所述第一专用网的网络地址被包括在所述第二专用网的网络地址之内，或者反之亦然，则所述控制单元生成一个新的网络地址表，以便所述第一和所述第二专用网在所述 VPN 隧道中使用不同的网络地址，和基于所述新的网络地址表变换地址，并且转发从所述第一专用网或者从连接到所述第二专用网的主机发送的数据分组。

2. 根据权利要求 1 的网关，其中所述控制单元包括:

一个 web 服务器，用于提供一个隧道建立请求页，以便连接到所述第一专用网的主机请求隧道的建立;

一个专用网域名服务器(DNS)处理器，用于对由所述连接到所述第二专用网的主机提出的所述隧道建立请求，从连接到所述公共网络的域名服务器(DNS)获得一个所述第二专用网的网关的网际协议(IP)地址;

一个虚拟本地网(VPN)处理器，按照经由所述至少一个或多个公共网络接口，或者经由所述至少一个或多个本地网接口传送的所述隧道建立请求作为服务器或者客户机而操作，并且生成一个到所述第二专用网的隧道；和

一个 NAT / NAPT 处理器，用于对从所述专用网发送到所述公共网络的数据分组，或者反之亦然，通过使用一个网络地址端口变换(NAPT)协议，变换一个专用 IP 地址为一个 IP 地址，或者变换一个 IP 地址为一个专用 IP 地址，其中，

如果一个 VPN 隧道在所述第一专用网和所述第二专用网之间被建立，则在所述 VPN 隧道中通过使用一个网络地址变换(NAT)协议变换专用 IP 地址。

3. 根据权利要求 2 的网关，其中，如果所述隧道建立请求从连接到所述第一专用网的所述主机被发送，则所述 VPN 处理器发出所述隧道建立请求消

息给所述第二专用网的网关，以及，

如果一个对于所述隧道建立请求的响应从所述第二专用网的网关被接收，则所述 VPN 处理器发出一个确认(ACK)给所述第二专用网的网关。

4. 根据权利要求 3 的网关，其中所述隧道建立请求消息包括一个所述第二专用网的网络地址，和一个在 VPN 隧道中将被用于所述第二专用网的网络地址的第二网络地址。

5. 根据权利要求 3 的网关，其中，如果所述包括一个所述第二专用网的网络地址，以及一个在 VPN 隧道中作为所述第二专用网的网络地址使用的第二网络地址的隧道建立请求消息被接收，则所述 VPN 处理器发送给所述第二专用网一个响应消息，该响应消息包括所述第一专用网的网络地址，所述第二网络地址，和一个在 VPN 隧道中作为所述第二专用网的网络地址使用的第三网络地址。

6. 根据权利要求 2 的网关，其中所述 web 服务器可以由一个中间件服务器来替换。

7. 根据权利要求 1 的网关，其中所述控制单元包括:

一个 web 服务器，用于提供一个隧道建立请求页，以便让连接到所述第一专用网的主机请求隧道的建立;

一个专用网域名服务器(DNS)处理器，用于对由连接到所述第一专用网的所述主机提出的所述隧道建立请求，从连接到公共网络的域名服务器(DNS)获得一个所述第二专用网的网关的网际协议(IP)地址;

一个本地到本地隧道启动协议(HTIP)处理器，用于按照经由所述至少一个或多个公共网络接口发送的，或者经由所述至少一个或多个本地网接口发送的所述隧道建立请求，发送和接收一个隧道建立请求消息，所述隧道建立请求消息包含用于所述第一和所述第二专用网之间隧道建立所必要的参数;

一个虚拟本地网(VPN)处理器，作为服务器或者客户机而操作，并且处理使得所述隧道可以在所述第一和所述第二专用网之间被建立；和

一个 NAT / NAPT 处理器，用于对从所述专用网发送到所述公共网络的数据分组，或者反之亦然，通过使用一个网络地址端口变换(NAPT)协议，变换一个专用 IP 地址为一个 IP 地址，或者变换一个 IP 地址为一个专用 IP 地址，其中，

如果一个 VPN 隧道被建立在所述第一专用网和所述第二专用网之间，并

且如果需要地址变换，则所述 NAT / NAPT 处理器通过使用一个网络地址变换(NAT)协议在所述 VPN 隧道中变换专用 IP 地址。

8. 根据权利要求 7 的网关，其中，如果到所述第二专用网的所述隧道建立请求被从连接到所述第一专用网的所述主机接收，则所述 HTIP 处理器发送所述隧道建立请求消息到所述第二专用网的网关，以及，

如果一个对于所述隧道建立请求的响应从所述第二专用网的网关被接收，则所述 HTIP 处理器发送一个确认(ACK)消息给所述第二专用网的网关。

9. 根据权利要求 8 的网关，其中包括在到所述第二专用网的所述隧道建立请求消息中的所述参数包括:

一个在建立隧道中使用的 VPN 协议;

一个所述第一专用网的网络地址; 和

在所述 VPN 隧道中作为所述第一专用网的网络地址使用的第二网络地址。

10. 根据权利要求 8 的网关，其中，如果所述隧道建立请求消息从所述第二专用网被接收，则所述 HTIP 处理器发出一个响应消息，

所述隧道建立请求消息包括一个在建立隧道中使用的 VPN 协议，一个所述第二专用网的网络地址，和在所述 VPN 隧道中作为所述第二专用网的网络地址使用的第二网络地址，以及，

所述响应消息包括一个在建立隧道中使用的 VPN 协议，一个所述第一专用网的网络地址，在所述 VPN 隧道中用于所述第一专用网的网络地址的第三网络地址，一个所述第二专用网的网络地址，和所述第二网络地址。

11. 根据权利要求 8 的网关，其中，如果所述 ACK 消息被从所述第二专用网接收，则所述 HTIP 处理器设置所述 VPN 处理器为一个 VPN 服务器，并且发出一个 READY 消息，通知所述第二专用网所述 VPN 处理器的设置已经完成。

12. 根据权利要求 11 的网关，其中，如果所述 READY 消息被从所述第二专用网接收，则所述 HTIP 处理器相对于所述第二专用网的 VPN 服务器设置所述 VPN 处理器为一个 VPN 客户机，并且驱动所述 VPN 客户机以在所述第一专用网和所述第二专用网之间建立一个 VPN 隧道。

13. 根据权利要求 8 的网关，其中所述 HTIP 处理器分析来自所述第二专用网的所述隧道建立请求消息或者所述响应消息，并且如果确定所述消息是

不合适的，则因此通过发出一个 NAK 消息给所述第二专用网来通知该同一情况。

14. 根据权利要求 13 的网关，其中，如果响应所述隧道建立请求消息，或者被发送给所述第二专用网的所述响应消息的所述 NAK 消息被接收，则所述 HTIP 处理器重新设置包含在所述消息中的参数和参数值，并且重新发送所述重新设置的参数和参数值给所述第二专用网。

15. 根据权利要求 8 的网关，其中所述 HTIP 处理器预先协商参数，该参数包括一个在建立隧道中使用的 VPN 协议，一个所述第一专用网的网络地址，一个在所述 VPN 隧道中用于所述第一专用网的网络地址的第二网络地址，一个所述第二专用网的网络地址，一个在所述 VPN 隧道中用于所述第二专用网的网络地址的第三网络地址，以便当在已有 VPN 隧道中使用的网络地址不和所述 VPN 隧道的网络地址相冲突时，VPN 隧道在所述至少一个或多个专用网之中被同时建立。

16. 根据权利要求 7 的网关，其中所述 web 服务器可以由一个中间件服务器来替换。

用于在不同的专用网的网络设备之间支持通信的网关

技术领域

本发明涉及一种网关，特别涉及一种用于在连接到不同的网络的网络设备之间支持通信的网关。

背景技术

随着通信技术的最新发展，高速数据服务网络被广泛普及。面对这样的背景，越来越多的公司开发和制造具有联网功能的数字信息家用器具，诸如冰箱、数字 TV 和可连接到该因特网的机顶盒。由于这些家用器具能够起具有增加其网络功能的信息终端的作用，所以已经开发了一种新的形式的网络，即本地网络。

在家庭中，形成一个本地网络的电动/电子产品以有线/无线方式连接到因特网，使得无论他/她位于何处，诸如本地，远程位置等等，用户都可以经由因特网发送与接收信息和控制电动/电子产品。

为了连接电动/电子产品到因特网，新型的网络设备在家庭中借助于必要的嵌入式程序而建立。在网络设备中，一个本地网关起连接本地网络与因特网的作用，并且控制网络数据分组的流量。

当前，每个家庭通过使用基本的本地网关，诸如 ADSL 和电缆调制解调器，得到从一个连接到因特网的因特网服务提供者(ISP)给出一个公用的网际协议(IP)地址。

这些常规的本地网关提供一种简单的连接服务，其连接一个本地网络到因特网。同时，近来的趋势要求经由本地网关提供的各种各样的服务，因为多个网络设备能够在家庭中使用，小型办公室本地交易(SOHO)和室内工作的广泛普及，以及装置自动化与远程控制被积极地开发。但是，该常规的本地网关不能满足当前的需要。

为了满足用户的需要，已经提出了一种本地网络使用专用 IP 地址的方法。这种方法将网络地址端口变换(NAPT)技术应用到一个本地网关，以便本地网络的多个网络设备以一个共享 IP 地址访问该因特网。

问题是本地网关的IP地址频繁地变化，因此每当他/她想要连接到与因特网相连接的本地网络时，需要用户去查找当前的IP地址。为了解决这个问题，已经提出了一种技术，其中一个本地网关被从ISP给出一个IP地址，然后该本地网关的域名和分配的IP地址被注册到因特网上的一个动态的DNS服务器中。据此，该用户可以经由域名而不是IP地址访问在他或者她的家庭中的设备。

一个本地网关被从ISP给出一个IP地址，但是，由于多个信息设备在家庭中在本地网络环境下使用，所以存在一个问题，即，设备不能同时以共享的IP地址连接到因特网。因此，专用IP地址在本地被使用，并且通过使用一个共享的IP地址连接信息设备到因特网的NAPT技术也被使用。

如果存在从本地到因特网的数据分组，则该NAPT变换一个数据分组源的专用IP地址和一个源端口编号为一个分配的IP地址和一个不同的端口编号，其被记录在一个NAPT变换表中。如果响应上述的数据分组被从该因特网发送到一个本地网络，则该本地网关参考该NAPT表，变换一个数据分组目标的IP地址和一个目标端口编号为一个专用IP地址和一个端口编号，并且转发该响应数据分组到最后的目标。如果从因特网转发给本地网络的数据分组没有被记录在该NAPT表中，则该数据分组被丢弃。

该NAPT技术的使用使从本地网络能够访问因特网。也就是说，在一个专用网上的多个网络设备可以通过共享一个IP地址来访问因特网。但是，如果对于网络设备从因特网访问本地网络则不可能，这是因为不能预先知道诸如专用IP地址和端口，本地网关端口编号，IP地址和端口，以及IP协议的信息，这些信息被记录在该NAPT表中，以便由一个接入到因特网的外部用户发送的数据分组经由一个本地网关被变换并路由到专用网之内。

该VPN是一种应用于本地网关的技术，用于使一个接入到因特网的用户能够从外界访问网络设备。VPN可以取决于环境和施加的网络分级结构而改变，但是，在本地网络环境中，2层隧道协议，诸如PPTP和L2TP被广泛地使用。每个本地网关具有一个VPN服务器，并且一个连接到因特网的远程用户起一个VPN客户机的作用。每个本地网络的本地网关可以在每个本地网络中起一个VPN服务器或者一个VPN客户机的作用。首先，一个VPN客户机请求VPN服务器通过使用一个IP地址在因特网上建立一个隧道。如果该隧道被建立起来，则该VPN服务器验证VPN客户机，并且分配给该VPN客户

机一个该客户机可以在本地网络之内使用的专用 IP 地址。该 VPN 客户机通过使用分配的专用 IP 地址生成一个虚拟网络接口，并且该接口被连接到该本地网络，并且起一个网络的作用。该 VPN 客户机的 IP 地址被用于去建立一个到该 VPN 服务器的隧道，并且该专用 IP 地址在经由隧道被连接的本地网络中使用。

如上所述，应用到本地网关的 NAPT 和 VPN 技术使得能够经由在家庭处的多个网络设备连接到因特网，以及能够将在因特网上的远程用户连接到本地网络。

但是，以上所述的技术，诸如 NAPT 和 VPN 连接本地网络与因特网，有一个问题，即它们无法在一个任意的本地网络和另一个本地网络之间提供连接。因为一个本地网络使用专用 IP 地址，使用不同的 IP 地址的多个本地网络可以同时使用相同的专用 IP 地址。如果一个连接到本地网络的主机传送数据，并且属于该本地网络的主机与属于远程本地网络的主机一样具有相同的 IP 地址，那么当数据传输时，由于不能判定数据是否被传送到属于哪一个本地网络的一个设备，所以会出现错误。

发明内容

为了解决上述的缺点及其他与常规配置有关的问题，已经开发了本发明。本发明的一个方面是提供一种支持在连接到不同的专用网的网络设备之间通信的网关。

本发明的上述的方面和/或其他的特点实际上是通过提供一种网关实现的，该网关包括：至少一个或多个连接到公共网络的公共网络接口；至少一个或多个连接到专用网的本地网接口；和一个控制单元。如果一个隧道建立请求被从一个连接到第一专用网的主机接收，去建立一个到正连接公共网络的第二专用网的隧道，则控制单元通过与第二专用网的网关通信来建立一个 VPN 隧道。如果第二专用网和第一专用网具有相同的网络地址，或者如果该第一专用网的网络地址被包括在第二专用网的网络地址中，或者反之亦然，则该控制单元会生成一个新的网络地址表，以便该第一和第二专用网在 VPN 隧道中可以使用不同的网络地址，并且基于新的网络地址表变换地址，而转发从第一专用网或者从连接到第二专用网的主机发送的数据分组。

控制单元包括：一个 web 服务器，用于提供一个隧道建立请求页，以便

连接到第二专用网的主机请求建立该隧道；一个专用网域名服务器(DNS)处理器，用于对于由连接到第二专用网的主机请求的到第一专用网的隧道建立，从连接到公共网络的 DNS 获得一个第一专用网的网关的网际协议(IP)地址；一个虚拟本地网(VPN)处理器，按照经由公共网络接口，或者经由本地网接口传送的隧道建立请求，起一个服务器或者客户机的作用，并生成一个到第一专用网的隧道；和一个 NAT / NAPT 处理器，用于相对于从第一专用网发送到公共网络的数据分组，或者反之亦然，通过使用一个网络地址端口变换(NAPT)协议，变换一个专用 IP 地址为一个 IP 地址，或者变换一个 IP 地址为一个专用 IP 地址。如果一个 VPN 隧道在第一专用网和第二专用网之间被建立，则控制单元在 VPN 隧道中通过使用一个网络地址变换(NAT)协议来变换专用 IP 地址。该 web 服务器可以用一个中间件服务器替换。

如果隧道建立请求是从连接到该第一专用网的主机发送到第二专用网的，则该 VPN 处理器将该隧道建立请求消息发送给第二专用网的网关，该隧道建立请求消息包括第一专用网的网络地址和在 VPN 隧道中被作为第一专用网的网络地址使用的第二网络地址。如果一个对于隧道建立请求的响应从第二专用网的网关被接收到，其包括该第二专用网的网络地址、第二网络地址和在 VPN 隧道中被作为第二专用网的网络地址使用的第三网络地址，则该 VPN 处理器发送一个确认(ACK)给该第二专用网的网关，该确认(ACK)包括第一专用网的网络地址，第二专用网的网络地址，第二网络地址和第三网络地址。VPN 处理器通过从到第二专用网的隧道建立请求消息的产生直到发送该 ACK 消息为止过程，生成一个专用网连接管理表。该专用网连接管理表包括： 第一专用网的网络地址，第二专用网的网络地址，第二网络地址，和第三网络地址，并且可以进一步包括：第二专用网的网关的域名，和按照第二专用网的网关的 VPN 操作的服务器/客户机状态显示项目。

如果该 VPN 处理器产生专用网连接管理表，则该 NAT / NAPT 处理器为连接到专用网的主机建立网络地址变换(NAT)。

如果一个对连接到第二专用网的第二主机的通信请求，在建立了到第二专用网的 VPN 隧道的状态中，从连接到第一专用网的第一主机传送，则该 DNS 处理器向第二专用网的网关询问有关该第二主机的第三网络地址。如果对于有关第二主机的第三网络地址的询问的一个响应从第二专用网的网关接收到，则该 DNS 处理器发送一个第二主机的第三网络地址到第一主机。

如果将以第二主机的第三网络地址作为目的地的地址的数据分组从第一主机传送，则该控制单元经由 VPN 隧道转发该数据分组到第二专用网的网关。

如果包括第二专用网的网络地址和作为在 VPN 隧道中第二专用网的网络地址使用的第二网络地址的隧道建立消息被接收，则该 VPN 处理器发送给第二专用网一个响应消息，该响应消息包括一个第一专用网的网络地址，第二网络地址，和作为在 VPN 隧道中第一专用网的网络地址使用的第三网络地址。VPN 处理器通过从接收来自第二专用网的隧道建立请求消息，直到接收到一个响应该响应消息的 ACK 消息为止的处理过程，生成一个专用网连接管理表。该专用网连接管理表包括该第一专用网的网络地址，第二专用网的网络地址，第二网络地址和第三网络地址，并且可以进一步包括：一个第二专用网的网关的域名，和一个按照第二专用网的网关的 VPN 操作的服务器/客户机状态显示项目。

如上所述，当 VPN 处理器生成专用网连接管理表时，NAT / NAPT 处理器参考该专用网连接管理表，为连接到专用网的主机建立一个网络地址变换(NAT)。

如果一个进入连接到第二专用网的主机之内的询问从第一专用网被接收，作为响应，DNS 处理器发送一个在 VPN 隧道中使用的主机的网络地址。

如果具有主机的第三网络地址作为目的地地址的数据分组从第二专用网被传送，则该控制单元参考 NAT，将已接收的数据分组发送到该主机。

控制单元包括：一个 web 服务器，用于提供一个隧道建立请求页，以便为连接到第一专用网的主机请求建立该隧道；一个专用网域名服务器(DNS)处理器，用于对连接到第一专用网的主机的隧道建立请求；从连接到公共网络的域名服务器(DNS)获得第二专用网的网关的网际协议(IP)地址；一个本地到本地隧道启动协议(HTIP)处理器，用于按照经由公共网络接口发送的或者经由本地网接口发送的隧道建立请求，发送和接收一个隧道建立请求消息，该隧道建立请求消息包含用于在第一和第二专用网之间建立隧道必需的参数；一个虚拟本地网(VPN)处理器，起一个服务器或者客户机的作用，并且处理使得隧道能够在第一和第二专用网之间被建立；和一个 NAT / NAPT 处理器，用于对从专用网发送到公共网络的数据分组，或者反之亦然，通过使用网络地址端口变换(NAPT)协议，变换一个专用 IP 地址为一个 IP 地址，或者

变换一个 IP 地址为一个专用 IP 地址。如果一个 VPN 隧道在第一专用网和第二专用网之间被建立，并且如果地址变换是需要的，则该 NAT / NAPT 处理器通过使用一个网络地址变换(NAT)协议变换在该 VPN 隧道中的专用 IP 地址。该 web 服务器可以由一个中间件服务器替换。

如果对第二专用网隧道建立请求是从连接到第一专用网的主机接收到的，则该 HTIP 处理器发送该隧道建立请求消息给第二专用网的网关。该隧道建立请求消息可以包括一个在隧道中使用的 VPN 协议，第一专用网的网络地址和在 VPN 隧道中使用的第二网络地址，而不是第一专用网的网络地址。当 HTIP 处理器从第二专用网的网关接收一个对于该隧道建立请求的响应的时候，该 HTIP 处理器发送给第二专用网的网关一个确认(ACK)。该响应可以包括一个在隧道中使用的 VPN 协议，第二专用网的网络地址，在 VPN 隧道中使用的第三网络地址，而不是第二专用网的网络地址，第一专用网的地址，和在 VPN 隧道中使用的第二网络地址，而不是第一专用网的网络地址，并且该 ACK 可以包括 VPN 协议，第一专用网的网络地址，第二专用网的网络地址，第二网络地址，和第三网络地址。 当接收到一个 READY 消息的时候，HTIP 处理器设置 VPN 处理为一个 VPN 客户机，并且使该 VPN 客户机被驱动，该 READY 消息包括一个在隧道中使用的 VPN 协议，在该 VPN 隧道中使用的第三网络地址，而不是第二专用网的网络地址，第一专用网的地址，和在 VPN 隧道中使用的第二网络地址，而不是第一专用网的网络地址。

通过经历从对第二专用网的隧道建立请求消息生成的，直到接收到 READY 消息为止的处理过程，该 HTIP 处理器产生一个专用网连接管理表。该专用网连接管理表可以包括第一专用网的网络地址，隧道的 VPN 协议，隧道的 ID，第二专用网的网络地址，第二网络地址和第三网络地址，并且可以进一步包括第二专用网的网关的域名，和按照第二专用网的网关的 VPN 操作，显示服务器/客户机状态的服务器/客户机状态显示项目。

VPN 隧道在第一和第二专用网之间被形成，并且如果在该 VPN 隧道的两端上都需要地址变换，则该 HTIP 处理器控制该 NAT / NAPT 处理器，使得可以参考专用网连接管理表，在该 VPN 隧道的两端上设置地址变换。

在 VPN 隧道在第一和第二专用网之间被建立的状态下，如果一个通信请求从第一专用网的第一主机被发送到第二专用网的第二主机，则该 DNS 处理器询问第二专用网的网关有关对应于该第二主机的域名的 IP 地址。如果从第

二专用网的网关接收一个响应，则该 DNS 处理器发送该接收的响应给第一主机。

如果指定给第二主机的 IP 地址的数据分组被从第一主机发送，则控制单元经由 VPN 隧道转发该数据分组到第二专用网的网关。

如果从该第二专用网接收一个隧道建立请求消息，则该 HTIP 处理器发送一个响应消息给第二专用网。隧道建立请求消息可以包括一个隧道的 VPN 协议，一个第二专用网的网络地址，和在 VPN 隧道中使用的第二网络地址，而不是第二专用网的网络地址，而响应消息可以包括该隧道的 VPN 协议，第一专用网的网络地址，在 VPN 隧道中使用的第三网络地址，而不是第一专用网的网络地址，第二专用网的网络地址和第二网络地址。

如果从第二专用网接收 ACK 消息，则该 HTIP 处理器设置 VPN 处理器为一个 VPN 服务器，并且发送一个 READY 消息给第二专用网的网关。该 READY 消息可以包括一个隧道的 VPN 协议，一个第一专用网的网络地址，一个在 VPN 隧道中使用的第三网络地址，而不是第一专用网的网络地址，一个第二专用网的网络地址，和一个在 VPN 隧道中使用的第二网络地址，而不是第二专用网的网络地址。

通过经历从第二专用网接收隧道建立请求消息，直到响应该响应消息的 READY 消息的传输为止的处理过程，该 HTIP 处理器产生一个专用网连接管理表。该专用网连接管理表可以包括一个隧道的 VPN 协议，一个隧道的 ID，一个第一专用网的网络地址，一个第二专用网的网络地址，第二网络地址和第三网络地址，并且可以进一步包括一个第二专用网的网关的域名，和按照第二专用网的网关的 VPN 操作，去显示服务器/客户机状态的服务器/客户机状态显示项目。

如果在第一和该第二专用网之间形成一个 VPN 隧道，并且在 VPN 隧道的两端都需要一个地址变换，则该 HTIP 处理器控制 NAT / NAPT 处理器，使得可以参考该专用网连接管理表，在 VPN 隧道的两端设置地址变换。

如果从第二专用网接收到一个关于连接到第一专用网的主机的询问，则该 DNS 处理器作为响应发送一个在 VPN 隧道中使用的主机的网络地址。

如果去往该主机的第三网络地址的数据分组从第二专用网被发送，则该控制单元参考 NAT / NAPT 处理器的变换表，变换该数据分组的目的地地址，并且发送该数据分组给该主机。

按照如上所述的本发明的某个实施例的网关能够使从专用网到公共网络(因特网)联网，以及使从因特网到专用网联网，包括使从一个专用网到不同的专用网联网，因此用户可以更大的扩展网络范围。

附图说明

通过参考附图描述本发明的某些实施例，本发明上述的方面和特点将更加清楚，其中：

图 1 是一个示出按照本发明的一个实施例的包括网关的网络结构图；

图 2 是一个图 1 的网关的示意性方框图；

图 3 是一个用于解释在二个具有不同的扩展网络 ID 的专用网之间建立一个 VPN 隧道的信号流程图；

图 4 是一个信号流程图，用于解释通过图 3 的处理过程，经由一个在专用网 A 和专用网 B 之间的隧道，在主机 A 和 B 之间数据分组的传送过程；

图 5 是一个用于解释具有相同的扩展网络 ID 的二个专用网的 VPN 隧道建立过程的信号流程图；

图 6 是一个信号流程图，用于解释通过图 5 的处理过程，经由一个在专用网 A 和专用网 B 之间建立的隧道，在主机 A 和主机 B 之间数据分组的传送过程；

图 7 是一个信号流程图，用于解释当专用网 A 的扩展网络 ID 被包括在专用网 B 的扩展网络 ID 中时，在二个专用网之间的 VPN 隧道建立过程；

图 8 是一个按照本发明另一个实施例的网关的示意性方框图；

图 9 是一个用于解释具有不同的扩展网络 ID 的两个专用网之间 VPN 隧道建立过程的信号流程图；

图 10 是一个信号流程图，用于解释通过在图 9 中示出的过程，经由在其间建立的隧道，在主机 A 和主机 B 之间数据分组的传送过程；

图 11 是一个用于解释在具有彼此相配的扩展网络 ID 的两个专用网之间的 VPN 隧道建立过程的信号流程图；

图 12 是一个信号流程图，用于解释通过在图 11 中示出的过程，经由在其间建立的隧道，在主机 A 和主机 B 之间数据分组的传送过程；和

图 13 是一个信号流程图，用于解释当专用网 A 的扩展网络 ID 被包括在专用网 B 的扩展网络 ID 中时，在二个专用网 A 和 B 之间的 VPN 隧道建立过

程。

具体实施方式

参考附图将更详细地描述本发明的某些实施例。

在下面的说明中，甚至在不同的附图中，相同的附图参考数字被用于相同的单元。在说明书中定义的内容，诸如详细的结构和单元只是提供帮助全面地理解本发明。因此，很明显，无需那些限定的内容也可以实现本发明。此外，公知的功能或者结构不做详细描述，因为多余的详述将使本发明难以理解。

另外，在该说明书中，单个的参考数字可用于表示多个单元。

图 1 是一个示出按照本发明一个实施例的包括本地网关的网络结构图。该网络包括专用网 200A 和 200B、接入网络和因特网 300。该专用网 200A 和 200B 分别地具有连接在其中的专用网主机 210A 和 210C 以及专用的主机 210B 和 210D，和一个 DNS 服务器 330 以及多个连接到因特网 300 的公共网络主机 310 和 320。该专用网 200A 和 200B 和因特网 300 经由包括 ISP 150 和本地网关 100A 和 100B 的接入网络而相互连接。

连接专用网 A 和 B (200A 和 200B)和因特网 300 的本地网关 A 和 B (100A 和 100B)的每一个分别从每个的 ISP 150 分配一个 IP 地址，并且登记该分配的 IP 地址到连接因特网的 DNS 服务器 330。每个本地网关 A 和 B (100A 和 100B)通过一个 NAPT 协议和一个 VPN 提供服务，使得在每个专用网上的主机 A、B、C 和 D (210A、210B、210C 和 210D)可以和连接到因特网 300 的主机 310 和 320 相互通信。此外，本地网关 100 提供服务，以便在专用网 A 和 B (200A 和 200B)的其中一个上的主机 A 和 C (210A 和 210C)与连接到专用网 A 和 B (200A 和 200B)的另一个上的主机 B 和 D (210B 和 210D)相互通信。因此，一旦当一个连接请求从在专用网 A (例如，200A)上的一个主机(例如，主机 A)传送到专用网 B (例如，200B)的另一个主机(例如，主机 B)时，本地网关 A (100A)建立一个用于通信的到对方本地网关 B (100B)的 VPN 隧道，用于 VPN 隧道的不同的专用 IP 地址被分配给连接到相应的专用网 A 和 B (200A 和 200B)的主机 210，使得在该隧道的两端，连接到专用网 A (例如，200A)的主机 A (例如，210A)或者主机 C (例如，210C)可以经由 NAT 与连接到专用网 B (例如 200B)的主机 B (例如，210B)或者主机 D (例如，210D)相互

通信。

图 2 是一个用于示出按照本发明一个实施例的网关的方框图。每个网关 100 包括一个公共网络接口 110，一个本地网接口 120，一个存储单元 130 和一个控制单元 140。

如上所述提供至少两个或更多的接口，并且它们中的至少一个是公共网络接口，以及它们中的至少一个是本地网接口。该公共网络接口 110 实际上通过 ADSL、电缆调制解调器或者以太网物理上连接到因特网 300，并且具有一个从 ISP 150 分配的 IP 地址。本地网接口 120 可以借助于以太网、无线局域网或者本地 PNA 以有线和/或无线方式配置，并且该控制单元 140 具有专用 IP 地址。用于一个专用网的网络地址是随机地从由因特网号码分配管理组(IANA)允许使用的地址当中选择的。

存储单元 130 存储与系统操作相关的程序和新近产生和更新的数据。

控制单元 140 具有一个 NAT / NAPT 处理器 141，一个网际协议(IP)处理器 142，一个域名服务(DNS)处理器 143，一个动态主机配置协议(DHCP)处理器 144，一个路由器 145，一个 VPN 处理器 146，一个 web/中间件服务器 147，一个加密处理器 148，和一个用户验证处理器 149。

NAT / NAPT 处理器 141 变换一个专用 IP 地址为一个用于从专用网到因特网，或者从因特网到专用网传送数据分组的 IP 地址，或者变换一个 IP 地址为一个专用的地址。此外，在那些专用网通过使用 VPN 隧道被相互连接的情况下，该 NAT / NAPT 处理器 141 使用该 NAT 协议，变换在一个 VPN 隧道中的地址。NAT / NAPT 处理器 141 连续地产生和更新存储单元 130 的 NAT 和 NAPT 表。

IP 处理器 142 处理一个从公共接口 110 和本地网接口 120 传送的 IP 数据包(或者一个 IP 信息包)。

路由器 145 在一个连接到公共网络的外部主机和连接到专用网的主机之间建立一个最佳的路径。该路由器 145 连续地产生和更新存储单元 130 的路由选择表。

DNS 处理器 146 管理用于在专用网之内的主机的域名和专用 IP 地址。此外，如果发生从专用网之内的主机到专用网之外的主机的询问，则该 DNS 处理器 146 从在因特网上的 DNS 服务器 330，或者位于另一个专用网的上一级上的本地网关获得答复以用于响应。该 NDS 处理器 146 管理一个与专用网之

内的主机相关的 DNS 表。

当专用网之内的网络设备启动的时候，DHCP 处理器 144 响应专用网之内的主机对于可利用的专用 IP 地址、网关地址、DNS 处理器地址等等的请求。该 DHCP 处理器 144 作为响应主机的请求的一部分，获得一个主机的域名，并且传送该获得的域名给该 DNS 处理器 146，以便产生和更新该 DNS 表。

web/中间件服务器 147 提供了一种方式，即，专用网的用户可以请求建立一个到不同的专用网的隧道。该用户可以通过使用一个 web 浏览器或者一个中间件客户机来请求该服务。

VPN 处理器 146 相对于在因特网上的主机起一个 VPN 服务器的作用，或者起能够连接到不同的专用网的一个 VPN 服务器或者一个 VPN 客户机的作用。 此外，如果一个在专用网之内的主机请求经由 web/中间件服务器 147 连接到不同的专用网，则该 VPN 处理器 146 通过与不同的专用网通信而建立一个 VPN 隧道，并且基于专用网的一个网络地址，在 VPN 隧道的末端建立一个 NAT。为连接到其他的专用网所需的信息是通过产生一个专用网连接管理表来管理的，并且在表中产生的数据被存储在存储单元 130 中。专用网连接管理表包括自身专用网(self-private)的网络地址，其他的专用网的网络地址，在 VPN 隧道中使用的自身专用网的网络地址，和在 VPN 隧道中使用的其他的专用网的网络地址，并且可以进一步包括按照对方专用网网关的域名和对方专用网网关的 VPN 操作的服务器/客户机状态显示项目。

加密处理器 148 加密在专用网和公共网络之间或者在专用网和另一个专用网之间通信的数据分组。

用户验证处理器 149 对于想要从公共网络访问专用网的外部用户，或者对于进入到专用网网关用于配置改变等等的用户执行一个验证处理。

当对不同的专用网建立一个 VPN 隧道的时候，上述的网关执行对应于如下三个情况中的每一个的操作。下面将参考图 1 描述各种情况。

第一，存在一种情况即专用网 A (例如，200A)和专用网 B (例如，200B)的扩展网络 ID (网络 ID 和子网掩码相乘)相互不同。例如，当专用网 A (例如，200A)的网络 ID 被设置为 10.0.0.0 / 24 和专用网 B (例如，200B)的网络 ID 被设置为 10.0.1.0/ 24 (情况 1)时，专用网 A (例如，200A)的扩展网络 ID 变为 10.0.0.x，并且专用网 B 的扩展网络地址变为 10.0.1.x，因此它们变得彼此不同。在这种情况下，专用网 A 和专用网 B 可以仅借助于 VPN 隧道的建立互

相通信。

第二，存在一种情况即专用网 A 和专用网 B 的扩展网络 ID 彼此相同(情况 2)。例如，当专用网 A 和专用网 B 的网络 ID 都被设置为 10.0.0.0 / 24 时，专用网 A (例如，200A)和专用网 B (例如，200B)的所有扩展网络 ID 变为 10.0.0.x，因此它们是彼此相同的。在这种情况下，当在专用网 A (200A)上的主机 A (例如，210A)试着发送数据分组到在专用网 B (200B)上的主机 B (例如，210B)时，如果主机 C (210C)具有与主机 B (210B)相同的 IP 地址，由于其不知道从主机 A (210A)传送的数据分组发送到哪里，主机 B (210B)还是主机 C (210C)，所以本地网关 A (100A)会产生一个传输差错，使得在二个专用网之间无法通信。因此，在这种情况下，一个新的 IP 地址被分配，其可以在一个在专用网 A (200A)和专用网 B (200B)之间建立的隧道中使用。例如，专用网 A 被分配一个网络地址 10.0.1.0 / 24，以及专用网 B 被分配一个网络地址 10.0.2.0 / 24，以及 NAT 在 VPN 隧道的两个末端上被执行。因此，从专用网 A (200A)观察在专用网 B (200B)上的主机 210B 和 210D，在专用网 B (200B)上的主机被判定具有网络地址 10.0.2.x，并且，当从专用网 B (200B)观察的时候，在专用网 A (200A)上的主机 210A 和 210C 被判定具有网络地址 10.0.2.y，使得可以在专用网 A (200A)的主机 210A 和 210C 和专用网 B (200B)的主机 210B 和 210D 之间进行相互通信。

第三，可能存在一种情况，即专用网 A 的网络 ID 被包括在专用网 B 的网络 ID 中。例如，当专用网 A (200A)被给定 10.0.0.0 / 24，而专用网 B (200B)被给定 10.0.0.0 / 16 (情况 3)时，专用网 A (200A)的扩展网络 ID 变为 10.0.0.x，而专用网 B (200B)的扩展网络 ID 变为 10.0.x.x，因此它们是彼此不同的，但是该 10.0.0.x 作为 10.0.x.x 的一部分而被包括。甚至在这种情况下，一个 VPN 隧道在专用网 A (200A)和专用网 B (200B)之间被建立，网络地址被分别以 10.0.1.0 / 24 和 10.1.0.0 / 16 分配给专用网 A (200A)和专用网 B (200B)，并且 NAT 在隧道的两个末端上被执行。因此，当从专用网 A (200A)观察的时候，看到在专用网 B (200B)上的主机具有地址 10.1.x.y，并且，当从专用网 B (200B)观察的时候，看到在专用网 A (200A)上的主机具有地址 10.0.1.z，以便专用网 A (200A)的主机可以与专用网 B (200B)的主机通信。

在上述三种情况中，专用网 A (200A)和专用网 B (200B)的不同扩展网络 ID 无需另外的配置，就能够仅经由在其间建立的 VPN 隧道进行通信。

下文中，将根据上述的三种情况来描述 VPN 隧道的生成和在两个专用网之间的数据分组传送过程。

图 3 是用于解释在两个具有不同的扩展网络 ID 的专用网之间建立 VPN 隧道的过程的一个信号流程图。首先，专用网 A（200A）的用户在由网关 A 的 web 服务器 147 提供的一个隧道建立请求页上，通过主机 A（210A）处的 web 浏览器 212 来请求建立到专用网 B(200B)的隧道，请求在专用网 A(200A)和专用网 B（200B）之间建立隧道的网关 A（100A）在因特网上经由 DNS 处理器 143，从 DNS 服务器 330 获取网关 B(100B)的 IP 地址(211.32.119.136)。接下来，网关 A（100A）在 VPN 处理器 146 中运行一个客户机程序，并且请求网关 B（100B）的 VPN 处理器 146'生成一个隧道。在请求在专用网之间建立隧道的消息中，包括专用网 A(200A)的网络地址 10.0.0.0/24，以及在 VPN 隧道中将被用于替代专用网 A（200A）的网络地址的网络地址（10.0.0.0/24，10.0.1.0/24，10.0.2.0/24，...）。同时，由于如果专用网 A（200A）和专用网 B（200B）的网络地址不同，则 NAT 在 VPN 隧道中就不是必需的，所以按照原状选择了专用网 A（200A）的地址 10.0.0.0/24，并且在专用网 A 和专用网 B 的扩展网络地址彼此相同的情况下，则从 10.0.1.0/24，10.0.2.0/24 中选择一个可用的网络地址。

如果来自网关 A（100A）的消息请求在专用网之间的生成隧道，则网关 B（100B）从 VPN 处理器 146 将在专用网之间隧道生成的响应消息传送到网关 A(100A)。在该响应消息中，包括专用网 B(200B)的网络地址 10.0.1.0/24，在 VPN 隧道中将被用于替代专用网 A（200A）的网络地址的网络地址 10.0.0.0/24，以及在 VPN 隧道中将被用于替代专用网 B（200B）的网络地址的网络地址 10.0.1.0/24，10.0.2.0/24，10.0.3.0/24 等。

接收响应消息的网关 A（100A）将一个专用网之间隧道建立的确认（ACK）传送到网关 B（100B）。该 ACK 包括专用网 A（200A）的网络地址 10.0.0.0/24，专用网 B（200B）的网络地址 10.0.1.0/24，在 VPN 隧道中用于专用网 A（200A）的网络地址的网络地址 10.0.0.0/24，以及在 VPN 隧道中用于专用网 B（200B）的网络地址的网络地址 10.0.1.0/24。这时，如果专用网 A（200A）的地址与在 VPN 隧道中用作专用网 A（200A）的网络地址的网络地址相同，则意味着在 VPN 隧道中没有出现 NAT，如果不相同，则意味着出现了 NAT。

在接收并传送 ACK 消息之后，分别在网关 A（100A）和网关 B（100B）中产生专用网连接管理表 132 和 132′。专用网连接管理表 132 包括对应网关的域名，一个表明对应网关是否是 VPN 服务器或 VPN 客户机的项目，专用网 A（200A）的网络地址，专用网 B（200B）的网络地址，在 VPN 隧道中将被用于专用网 A（200A）的网络地址的网络地址，在 VPN 隧道中将被用于专用网 B（200B）的网络地址的网络地址，等等。

网关 A（100A）产生的表包括网关 B（100B）的域名（网关 B），表明网关 B 是 VPN 服务器的一个项目（服务器），专用网 A 的网络地址（10.0.0.0/24），专用网 A 的网络地址（10.0.0.0/24），专用网 B 的网络地址（10.0.1.0/24），在 VPN 隧道中将被用于专用网 A 的网络地址的网络地址（10.0.0.0/24），在 VPN 隧道中将被用于专用网 B 的网络地址的网络地址（10.0.1.0/24）等等。

如上所述，如果一个 ACK 信号在两个专用网之间被交换，则在网关 A（100A）和网关 B（100B）之间生成 VPN 隧道，以及在隧道中建立一个 PPP 连接。之后，从主机 A（210A）传送到网关 A（100A）的 VPN 隧道末端的数据分组经由 PPP 连接被传送到网关 B（100B）的 VPN 隧道的末端。

图 4 是用于解释通过一个隧道在主机 A（210A）和主机 B（210B）之间的数据分组传送方法的信号流程图，该隧道在专用网 A（200A）和专用网 B（200B）之间通过图 3 的过程建立。首先，专用网 A（200A）的用户知道主机 B（210A）的域名，以及安装到主机 A（210A）中的应用程序将一个 DNS 询问传送到网关 A（100A），以获知对应于主机 B（210B）域名的 IP 地址。相应地，网关 A（100A）的 DNS 处理器 143 查询专用网连接管理表 132。如果一个 VPN 隧道在专用网 A（200A）和专用网 B（200B）之间被建立，则 DNS 处理器 143 将到主机 B（210B）的 DNS 询问发送到网关 B（100B）。此后，网关 A（100A）的 DNS 处理器 143 首先查询专用网连接管理表 132。此外，如果存在专用网 A（200A）和专用网 B（200B）之间建立的 VPN 隧道，则到主机 B（210B）的 DNS 询问被发送到网关 B（100B）。

如上所述，如果 DNS 询问从网关 A（100A）被传送到网关 B（100B），则网关 B（100B）的 DNS 处理器 143′将具有表明在 VPN 隧道中主机 B（210B）的网络地址 10.0.1.5 的响应消息传送到网关 A（100A），以代替主机 B（210B）的网络地址。

网关 A（100A）从网关 B（100B）的 DNS 处理器 143′将一个对应于主机 B（210B）的专用 IP 地址 10.0.1.5 转送到主机 A（210A）。

如果从网关 A（100A）接收主机 B（210B）的专用 IP 地址，则主机 A（210A）通过写入用于目地的地址的已接收专用 IP 地址（10.0.1.5）和用于源地址的主机 A（210A）的专用 IP 地址（10.0.0.4）而将数据分组传送到网关 A（100A）。

如果从主机 A（210A）接收到数据分组，则网关 A（100A）参考路由表 145 和转发设置，将已接收的数据分组传送到网关 A（100A）隧道的末端。由于 PPP 连接在网关 A（100A）和网关 B（100B）之间的 VPN 隧道中被设置，所以发送到网关 A（100A）的隧道末端的数据分组被传送到网关 B（100B）的隧道的末端。

如果数据分组经过 VPN 隧道被传送，则网关 B（100B）参考路由表 145′和转发设置将数据分组传送到主机 B（210B）。

如果数据分组被接收，则主机 B（210B）通过写入用于源地址的主机 B（210B）的一个专用 IP 地址（10.0.1.5）和用于目的地地址的主机 A（210A）的一个专用 IP 地址（10.0.0.4）来发送一个响应。

此后，主机 A（210A）和主机 B（210B）经过在专用网 A（200A）和专用网 B（200B）之间形成的隧道重复上述的数据分组传送过程。

图 5 是用于解释具有相同的扩展网络 ID 的两个专用网的 VPN 隧道建立过程的信号流程图。首先，如果专用网 A（200A）的用户在由网关 A（100A）的 web 服务器 147 提供的隧道建立请求页上，经过主机 A（210A）中的 web 浏览器 212 来请求建立到专用网 B（200B）的隧道，则接收用于在专用网 A（200A）和专用网 B（200B）之间建立隧道的一个请求的网关 A（100A），通过 DNS 处理器 143 在因特网上从 DNS 服务器 330 获得网关 B（100B）的 IP 地址（211.32.119.136）。接下来，具有获得的网关 B（100B）的 IP 地址的网关 A（100A）在 VPN 处理器 146 上运行一个客户机程序，并且请求网关 B（100B）的 VPN 处理器 146′在专用网之间生成一个隧道。请求在专用网之间建立隧道的消息包括专用网 A（200A）的网络地址（10.0.0.0/24），以及在 VPN 隧道中将被用于专用网 A 的网络地址的网络地址（10.0.0.0/24，10.0.1.0/24，10.0.2.0/24，…）。

如果从网关 A（100A）接收到一个隧道建立请求，则网关 B（100B）的

VPN 处理器 146′传送到网关 A（100A）一个对在专用网之间隧道建立请求的响应消息。该响应消息包括专用网 B（200B）的网络地址（10.0.0.0/24），以及在 VPN 隧道中用于专用网 A（200A）的网络地址的网络地址（10.0.1.0/24），以及在 VPN 隧道中用于专用网 B（200B）的网络地址的网络地址（10.0.2.0/24，10.0.3.0/24，10.0.4.0/24）。

如果接收到来自网关 B（100B）的响应消息，则网关 A（100A）就发送给网关 B（100B）一个在专用网之间隧道建立的 ACK。该 ACK 包括专用网 A（200A）的网络地址（10.0.0.0/24），专用网 B（200B）的网络地址（10.0.0.0/24），在 VPN 隧道中被用于专用网 A（200A）的网络地址的网络地址（10.0.1.0/24），以及在 VPN 隧道中将被用于专用网 B（200B）的网络地址的网络地址（10.0.2.0/24）。由于专用网 A（200A）的地址与在 VPN 隧道中用于专用网 A（200A）的网络地址的网络地址不一致，所以网关 A（100A）认识到通过 NAT 协议使用了地址变换。

在接收和传送 ACK 消息之后，专用网连接管理表 132 和 132′分别在网关 A（100A）和网关 B（100B）中产生。专用网连接管理表 132 包括对方网关 100 的域名，表明对应网关 100 是 VPN 服务器还是 VPN 客户机的一个项目，专用网 A（200A）的网络地址，专用网 B（200B）的网络地址，在 VPN 隧道中将被用于专用网 A（200A）的网络地址的网络地址，在 VPN 隧道中将被用于专用网 B（200B）的网络地址的网络地址，等等。

网关 A（100A）产生的表包括网关 B（100B）的域名（网关 B），表明网关 B 是 VPN 服务器的一个项目（服务器），专用网 A（200A）的网络地址（10.0.0.0/24），专用网 B（200B）的网络地址（10.0.0.0/24），在 VPN 隧道中被用于专用网 A（200A）的网络地址的网络地址（10.0.1.0/24），在 VPN 隧道中被用于专用网 B（200B）的网络地址的网络地址（10.0.2.0/24），等等。

通过上述的过程，网关 A（100A）和网关 B（100B）之间的一条 VPN 隧道被生成，并且在隧道中建立了一个 PPP 连接。此后，被发送到网关 A（100A）的 VPN 隧道末端的数据分组，通过 PPP 连接被传送到网关 B（100B）的 VPN 隧道末端。

如果生成了 VPN 隧道并且完成了 PPP 连接，那么网关 A（100A）就参考专用网连接管理表 132 来建立 VPN 隧道的网关 A（100A）的 NAT。如果 NAT 被建立，那么当数据分组通过网关 A（100A）从专用网 A（200A）被发

送到 VPN 隧道时，源地址 10.0.0.x 被变换成 10.0.1.x，以及当数据分组通过网关 A（100A）从 VPN 隧道被发送到专用网 A 时，目的地地址 10.0.1.y 被变换成 10.0.0.y。此外，网关 B 在 VPN 隧道的网关 B 处建立 NAT。

图 6 是一个信号流程图，用于解释在主机 A（210A）和主机 B（210B）之间通过一个隧道的数据分组传送方法，这个隧道是通过图 3 的过程在专用网 A 和专用网 B 之间建立的。首先，专用网 A（200A）的一个用户知道主机 B（210B）的域名，并且，如果安装在主机 A（210A）中的应用程序向网关 A（100A）发送一个对主机 B（210B）的 DNS 询问，则网关 A（100A）的 DNS 处理器 143 就查询专用网连接管理表 132。此外，如果在专用网 A（210A）和专用网 B（200B）之间建立一个 VPN 隧道，则为了获知在主机 B（210B）的 VPN 隧道中使用的专用 IP 地址，DNS 处理器 143 就向网关 B（100B）发送 DNS 询问，因为认识到 NAT 对于通过隧道的数据分组来说是必需的。

如果接收到对主机 B（210B）的询问，则网关 B（100B）的 DNS 处理器 143'向网关 A（100A）传送一个响应消息，该消息具有用于主机 B（210B）的 VPN 隧道中的 IP 地址，并且网关 A（100A）将它送回主机 A（210A）。

因此，为了将数据分组发送到主机 B（200B），主机 A（210A）将数据分组传送到网关 A（100A）。数据分组的目的地地址被写为 10.0.2.5，源地址被写为 10.0.0.4。

如果到主机 B（210B）的数据分组被从主机 A（210A）接收到，则网关 A（100A）参考路由表和转发设置将数据分组传送到网关 A 的隧道末端。因为在网关 A（100A）的 VPN 隧道末端处建立了 NAT，所以源地址 10.0.0.4 被变换成 10.0.1.4。由于为在网关 A（100A）和网关 B（100B）之间的隧道建立了 PPP 连接，所以具有通过 NAT 变换的源地址的数据分组被传送到网关 B（100B）的末端。

对于被传送到网关 B（100B）的隧道末端的数据分组来说，该网关 B（100B）具有通过上述 NAT 变换的源地址，网关 B（100B）通过建立在网关 B（100B）的 VPN 隧道末端上的 NAT 将目的地地址 10.0.2.5 变换成 10.0.0.5。参照路由表和转发设置，具有通过上述 NAT 变换的目的地地址的数据分组被传送到主机 B（210B）。

此后，主机 B（210B）发送一个响应到主机 A（210A），并且为了通信，重复上述的数据分组传送过程。

图 7 示出了一个信号流程图，用于解释在专用网 A 的扩展网络 ID 包括在专用网 B 的扩展网络 ID 中的情况下，在两个专用网之间的 VPN 隧道建立过程。首先，如果通过主机 A（210A）中的 web 浏览器 212，在由网关 A（100A）的 web 服务器 147 提供的一个隧道建立请求页上，专用网 A（200A）的一个用户向专用网 B（200B）请求隧道的建立，则接收用于在专用网 A（200A）和专用网 B（200B）之间建立隧道的请求的网关 A（100A），通过 DNS 处理器 143 从在因特网上的 DNS 服务器 330 获得网关 B（100B）的 IP 地址（211.32.119.136）。接下来，具有网关 B（100B）获得的 IP 地址的网关 A（100A）在 VPN 处理器 146 上运行一个客户机程序，并且请求网关 B（100B）的 VPN 处理器在专用网之间建立隧道。请求专用网之间建立隧道的消息包括专用网 A 的网络地址（10.0.0.0/24）和用于 VPN 隧道中专用网 A 的网络地址的网络地址（10.0.0.0/24，10.0.1.0/24，10.0.2.0/24，...）。

如果从网关 A（100A）接收到隧道建立请求消息，则网关 B（100B）的 VPN 处理器 146′就传送一个响应消息到在专用网间建立的隧道。该响应消息包括专用网 B（200B）的网络地址（10.0.0.0/16）和用于 VPN 隧道中本地网 A 的网络地址的网络地址（10.0.1.0/24），以及用于 VPN 隧道中专用网 B 的网络地址的网络地址（10.1.0.0/16，10.2.0.0/16，10.3.0.0/16，...）。

如果从网关 B（100B）接收到响应消息，则网关 A（100A）就向网关 B（100B）发送在专用网间建立隧道的一个 ACK。该 ACK 包括专用网 A（200A）的网络地址（10.0.0.0/24），专用网 B（200B）的网络地址（10.0.0.0/16），用于 VPN 隧道中专用网 A 的网络地址的网络地址（10.0.1.0/24），和用于在 VPN 隧道中专用网 B 网络地址的网络地址（10.1.0.0/24）。由于专用网 A 的地址与用于在 VPN 隧道中专用网 A 的网络地址的网络地址不一致，所以网关 A（100A）认识到使用了 NAT。

在接收和传送 ACK 消息后，专用网连接管理表 132 和 132′分别在网关 A（100A）和网关 B（100B）中产生。网关 A（100A）产生的表包括网关 B（100B）的域名，表明网关 B（100B）是 VPN 服务器的一个项目，专用网 A 的网络地址（10.0.0.0/24），专用网 B 的网络地址（10.0.0.0/16），用于 VPN 隧道中专用网 A 的网络地址的网络地址（10.0.1.0/24），用于 VPN 隧道中专用网 B 的网络地址的网络地址（10.1.0.0/16），等等。

通过上述过程，在网关 A（100A）和网关 B（100B）之间的 VPN 隧道

中建立了 PPP 连接。此后，发送到网关 A（100A）的 VPN 隧道末端的数据分组通过 PPP 连接被传送到网关 B（100B）的 VPN 隧道的末端。

接下来，如果 VPN 隧道被生成和 PPP 连接被完成，那么网关 A（100A）就参照专用网连接管理表 132，在 VPN 隧道的网关 A（100A）上建立 NAT。如果 NAT 被建立，则当数据分组通过网关 A（100A）被从专用网 A 发送到 VPN 隧道时，源地址 10.0.0.X 被变换成 10.0.1.X，而当数据分组通过网关 A（100A）从 VPN 隧道发送到专用网 A 时，目的地地址 10.0.1.y 被变换成 10.0.0.y。同样地，专用网 B（100B）也在 VPN 隧道的网关 B 上建立 NAT。

如果在上述的网关 A（100A）和网关 B（100B）之间形成的 VPN 隧道的两端上都建立了 NAT，则主机 A（210A）和主机 B（210B）就能通过图 6 所示的数据分组传送过程相互通信。

下面，将描述根据本发明的另一个实施例的网关。

图 8 是根据本发明另一个实施例的网关的框图。网关 100 包括公共网络接口 110，专用网接口 120，存储单元 130 和控制单元 140。

接口 110，专用网接口 120 和存储单元 130 具有与上面所描述的那些单元相同的操作和功能。控制单元 140 包括网络地址变换（NAT）/NAPT 处理器 141，网际协议（IP）处理器 142，域名服务（DNS）处理器 143，动态主机配置协议（DHCP）处理器 144，路由器 145，HTIP 处理器 146A，VPN 处理器 146B，web/中间件服务器 147，加密处理器 148 和用户验证处理器 149。

NAT/NAPT 处理器 141，IP 处理器 142，DNS 处理器 143，DHCP 处理器 144，路由器 145，web/中间件服务器 147，加密处理器 148 和用户验证处理器 149 具有与上面描述的那些部件相同的操作和功能。

HTIP 处理器 146A 协商用于在其它专用网之间的隧道生成的参数，相应地利用这些参数控制 VPN 处理器 146B 和 NAT/NAPT 处理器 141。有用的参数可能包括一种在 VPN 隧道生成中使用的 VPN 协议的类型，自专用网的网络地址，其它专用网的网络地址，在 VPN 隧道中使用的自专用网的网络地址，以及在 VPN 隧道中使用的其它专用网的网络地址。

HTIP 处理器 146A 使得能够在不考虑专用 IP 地址或所使用的 VPN 协议的类型，而实现在多个专用网的通信设备之间的直接通信。从协商中导出的参数，或者在专用网中生成的 VPN 隧道的列表被存储在存储单元 130 中。换句话说，对于与其它专用网连接所必需的信息，被列入专用网连接管理表中，

而该表格化的数据被存储在存储单元 130 中。

为了响应通过 web/中间件服务器 147 从专用网的主机传送的用于连接到另外一个专用网的请求，HTIP 处理器 146A 与其它的专用网通信，协商用于生成 VPN 隧道所必需的参数，根据已协商的参数来控制 VPN 处理器 146B 以生成 VPN 隧道，并控制 NAT/NATPT 处理器 141，以便能够根据专用网的网络地址在 VPN 隧道的末端设置 NAT。专用网连接管理表可以包括正被使用的 VPN 协议，自专用网的网络地址，另一个专用网的网络地址，在 VPN 隧道中被使用的自专用网的网络地址，在 VPN 隧道中被使用的另一个专用网的网络地址。另外，专用网连接管理表可以包括对方的专用网关的域名，以及根据对方的专用网关的 VPN 操作表明服务器/客户机状态的项目。

在作为 VPN 服务器或 VPN 客户机操作而使得能够与其它专用网连接的时候，VPN 处理器 146B 对位于因特网中的主机来将，起到服务器的作用。如果完成与位于其它专用网的网关中的 HTIP 处理器 146A'的协商，则 HTIP 处理器 146A 控制 VPN 处理器 146B 以便在不同的专用网间生成一个 VPN 隧道。

在其它专用网间形成 VPN 隧道的过程中，网关主要在三种情况中进行不同的操作，其包括，第一，当专用网 A（200A）具有来自专用网 B（200B）的不同扩展网络 ID 时，第二，当专用网 A（200A）具有与专用网 B（200B）相同的扩展网络 ID 时，以及第三，当专用网 A（200A）的网络 ID 被包括在专用网 B（200B）的网络 ID 中时。下面将参考上述三种情况详细描述生成 VPN 隧道和在两个专用网间传送数据分组的过程。

图 9 是一个信号流程图，其示出了在具有不同的扩展网络 ID 的两个专用网之间形成一个 VPN 隧道的过程。首先，专用网 A（200A）的用户通过 web 浏览器 212，在由网关 A（100A）的 web 服务器 147 提供的隧道建立请求页上，向专用网 B（200B）发送一个隧道建立请求。为了响应该请求，网关 A（100A）通过 DNS 处理器 143 从位于因特网中的 DNS 服务器 330 获取网关 B（100B）的一个公共 IP 地址 211.32.119.136。

接下来，网关 A（100A）在 HTIP 处理器 146A 上驱动 HTIP 程序，来请求网关 B（100B）的 HTIP 处理器 146A 建立一个隧道。专用网间的隧道建立请求可以包括将被使用的 VPN 协议，如 L2TP 以及在 VPN 隧道中用于替代专用网 A（200A）的网络地址的网络地址（10.0.0.0/24，10.0.1.0/24，

10.0.2.0/24，...）。如果专用网 A（200A）和专用网 B（200B）具有不同的网络地址，并且如果专用网 A（200A）的网络地址不是用于通过 VPN 隧道连接专用网 B（200B）和第三个专用网，因为在 VPN 隧道中不需要 NAT，所以直接选择专用网 A 的网络地址 10.0.0.0/24。如果专用网 A（200A）和专用网 B（200B）的扩展网络地址彼此相同，那么在地址 10.0.1.0/24，10.0.2.0/24，...中能够恰当地选择一个可用的地址。

一旦从网关 A（100A）接收到在专用网间建立隧道的请求，网关 B（100B）就通过 HTIP 处理器 146A 向网关 A（100A）发送一个隧道建立响应消息。该响应消息可以包括将被使用的 VPN 协议，如 L2TP，专用网 B（200B）的网络地址 10.0.1.0/24，在 VPN 隧道中用于替代专用网 B（200B）的网络地址的网络地址（10.0.1.0/24，10.0.2.0/24，10.0.3.0/24，...），专用网 A（200A）的网络地址 10.0.0.0/24，在 VPN 隧道中用于替代专用网 A（200A）的网络地址的网络地址 10.0.0.0/24。

一旦接收到该响应消息，网关 A（100A）就发送一个隧道建立 ACK 到网关 B（100B）。该 ACK 消息可以包括专用网 A（200A）的网络地址 10.0.0.0/24，专用网 B（200B）的网络地址 10.0.1.0/24，以及在 VPN 隧道中用于替代专用网 B（200B）的网络地址的网络地址 10.0.0.0/24。如果专用网 A（200A）的地址与 VPN 隧道中用于替代专用网 A（200A）的网络地址的网络地址相同，则 NAP 在 VPN 隧道中不出现，然而当网络地址彼此不匹配时出现 NAP。

在 ACK 消息被发送出去和接收到之后，专用网连接管理表 132 和 132′在网关 A（100A）和网关 B（100B）处被生成。专用网连接管理表 132 可以包括对方的网关的域名，被使用的 VPN 协议，如 L2TP，专用网之间的隧道 ID，表明对方的网关是 VPN 服务器还是客户机的一个项目，专用网 A（200A）的网络地址，专用网 B（200B）的网络地址，在 VPN 隧道中用于替代专用网 A（200A）的网络地址的网络地址，以及在 VPN 隧道中用于替代专用网 B（200B）的网络地址的网络地址。

由网关 A（100A）产生的表可以包括网关 B（100B）的域名，如‘网关 B’，表明网关 B 是 VPN 服务器的一个项目（服务器），专用网 A（200A）的网络地址 10.0.0.0/24，专用网 B（200B）的网络地址 10.0.1.0/24，在 VPN 隧道中用于替代专用网 A（200A）的网络地址的网络地址 10.0.0.0/24，以及在 VPN 隧道中用于替代专用网 B（200B）的网络地址的网络地址 10.0.1.0/24。

当接收到 ACK 消息时，根据将被使用的 VPN 协议，网关 B（100B）将 VPN 处理器 146B'设置成 VPN 服务器以便生成 VPN 隧道。如果隧道生成准备了包括将 VPN 处理器 146B'设置成 VPN 服务器的所有工作，则网关 B（100B）的 HTIP 的处理器 146A'向网关 A（100A）发送 READY 消息，从而通知在专用网之间的隧道生成的准备已经完成。READY 消息可以包括使用中的 VPN 协议，如 L2TP，专用网 A（200A）的网络地址 10.0.0.0/24，专用网 B（200B）的网络地址 10.0.1.0/24，在 VPN 隧道中使用的专用网 A（200A）的网络地址，以及在 VPN 隧道中使用的专用网 B（200B）的网络地址 10.0.1.0/24。

当接收到 READY 消息时，根据将被使用的 VPN 协议，网关 A（100A）将 VPN 处理器 146B 设置成网关 B(100B)的 VPN 客户机。HTIP 处理器 146A 驱动该 VPN 客户机，结果是在网关 A（100A）和网关 B（100B）之间建立了一个 VPN（L2TP）隧道。

如上所述，在两个专用网之间交换了 ACK 信号和 READY 信号后，一个 VPN 隧道被生成，并且从主机 A（210A）传送到网关 A（100A）的 VPN 隧道末端的数据分组被传送到网关 B（100B）的 VPN 隧道末端。

图 10 示出了通过在专用网 A（200A）和专用网 B（200B）之间形成的隧道，在主机 A（210A）和主机 B（210B）之间传送数据分组的过程的信号流程图。首先，专用网 A（200A）的一个用户知道主机 B（210B）的域名，并且安装在主机 A（210A）中的应用程序向网关 A（100A）发出一个 DNS 询问来找出与主机 B（210B）的域名相应的 IP 地址。相应地，网关 A（100A）的 DSN 处理器 143 查询专用网连接管理表 132。如果存在专用网 A（200A）和专用网 B(200B)之间建立的 VPN 隧道，则网关 A(100A)向网关 B(100B)发出关于主机 B（210B）的 DSN 询问。

当 DSN 询问从网关 A（100A）被传送到网关 B（100B）时，参照专用网连接管理表 132'，网关 B（100B）的 DSN 处理器 143'向网关 A（100A）发出一个响应消息。该响应消息包括表明 VPN 隧道中的主机 B（210B）的网络地址 10.0.1.5，而不是主机 B（210B）的网络地址。为了简明，发送 DSN 请求以及响应该请求的过程在附图中略去了。

网关 A（100A）向主机 A（210A）转发专用 IP 地址 10.0.1.5，其是从网关 B(100B)的 DNS 处理器 143'到主机 B(210B)的响应。当从网关 A(100A)

接收到主机 B（210B）的专用 IP 地址时，主机 A（210A）在目的地地址中写入接收到的专用 IP 地址 10.0.1.5，同时在源地址中写入主机 A（210A）的专用 IP 地址 10.0.0.4。据此，主机 A（210A）向网关 A（100A）发送数据分组。

当从主机 A（210A）接收到数据分组时，参照路由表 145 和转发设置，网关 A（100A）将接收到的数据分组传送到网关 A（100A）和网关 B（100B）之间形成的 VPN 的末端，以及发送到在网关 A（100A）的隧道末端的数据分组被传送到网关 B（100B）的隧道末端。

当通过 VPN 隧道传送该数据分组时，网关 B（100B）参照路由表 145′和转送设置将数据分组转送到主机 B（210B）。

当接收到该数据分组时，主机 B（210B）通过将主机 B（210B）的专用 IP 地址 10.0.1.5 写在目的地地址中，以及将主机 A（210A）的专用 IP 地址 10.0.0.4 写在目的地地址中，来处理所接收的数据分组和发出一个响应。

主机 A（210A）和主机 B（210B）连续重复上述的在本地网 A（200A）和本地网 B（200B）之间的数据分组传送过程。

图 11 示出了一个信号流程图，其中解释了在具有相同的扩展网络 ID 的两个专用网之间形成 VPN 隧道的过程。

首先，专用网 A（200A）的用户通过 Web 浏览器 212 从主机 A（210A）发送一个隧道建立请求页，其由网关 A（100A）的 Web 服务器 147 来提供，从而请求在专用网 A（200A）和专用网 B（200B）之间生成一个隧道。为了响应该请求以便在专用网 A（200A）和专用网 B（200B）之间形成一个隧道，网关 A（100A）通过 DNS 处理器 143 从位于因特网中的 DNS 服务器 330 获得网关 B（100B）的一个公共 IP 地址 211.32.119.136。为了简明，发送 DNS 询问和响应该询问的过程在附图中被忽略。

当网关 A（100A）获得网关 B（100B）的公共 IP 地址时，网关 A（100A）驱动在 HTIP 处理器 146A 中的 HTIP 程序，并且请求网关 B（100B）的 HTIP 处理器 146A′在专用网之间生成一个隧道。专用网之间的隧道建立请求可以包括将被使用的 VPN 协议，诸如 L2TP，专用网 A（200A）的网络地址 10.0.0.0/24，以及将在 VPN 隧道中用于代替专用网 A（200A）的网络地址的网络地址（10.0.0.0/24,10.0.1.0/24,10.0.2.0/24，…）。

当网关 B（100B）的 HTIP 处理器 146A′从网关 A（100A）接收一个隧道建立请求时，网关 B（100B）将一个对隧道建立请求的响应消息传送到网

关 A（100A）。该响应消息可以包括将被使用的诸如 L2TP 这样的 VPN 协议，专用网 B（200B）的网络地址（10.0.0.0/24），将在 VPN 隧道中代替专用网 B（200B）的网络地址的网络地址（10.0.2.0/24,10.0.3.0/24,10.0.4.0/24，...），专用网 A（200A）的网络地址（10.0.0.0/24）以及将在 VPN 隧道中代替专用网 A（200A）的网络地址的网络地址 10.0.1.0/24。

当网关 A（100A）从网关 B（100B）接收一个响应消息时，网关 A（100A）将一个 ACK 消息发送到网关 B（100B）。该 ACK 消息可以包括将被使用的诸如 L2TP 这样的 VPN 协议，专用网 A（200A）的网络地址 10.0.0.0/24，专用网 B（200B）的网络地址 10.0.0.0/24，将在 VPN 隧道中用于代替专用网 A（100A）的网络地址的网络地址 10.0.1.0/24，以及将在 VPN 隧道中用于代替专用网 B（200B）的网络地址的网络地址 10.0.2.0/24。因为在 VPN 隧道中代替专用网 A（200A）的网络地址使用的网络地址是不同的，所以网关 A（100A）认识到在 VPN 隧道的两端根据 NAT 协议进行了地址转换。

在交换了 ACK 消息之后，分别在网关 A（100A）和网关 B（100B）处生成专用网连接管理表 132 和 132`。每个专用网连接管理表 132 和 132`可能包括诸如 L2TP 这样的使用中的 VPN 协议，在专用网之间的隧道 ID，对方网关 100A 和 100B 的域名，表明对方的网关 100A 和 100B 是 VPN 服务器还是客户机的一个项目，专用网 A（200A）的网络地址，专用网 B（200B）的网络地址，将在 VPN 隧道中用于代替专用网 A（200A）的网络地址的网络地址，以及将在 VPN 隧道中代替专用网 B（200B）的网络地址的网络地址。

由网关 A（100A）产生的表可以包括诸如 L2TP 这样的使用中的 VPN 协议，诸如“网关 B”这样的网关 B（100B）的域名，表明网关 B 是 VPN 服务器的一个项目（一个服务器），专用网 A（200A）的网络地址 10.0.0.0/24，专用网 B（200B）的网络地址 10.0.0.0/24，将在 VPN 隧道中用于代替专用网 A（200A）的网络地址的网络地址 10.0.1.0/24，以及将在 VPN 隧道中用于代替专用网 B（200B）的网络地址的网络地址 10.0.2.0/24。

当网关 B（100B）接收 ACK 消息时，网关 B（100B）设置 VPN 处理器 146B`为一个 VPN 服务器，以便根据使用中的 VPN 协议生成 VPN 隧道。当完成在专用网之间的生成隧道的准备时，包括将 VPN 处理器 146B`设置为 VPN 服务器，网关 B（100B）的 HTIP 处理器 146A`发送 READY 消息到网关 A（100A），通知已经完成了在专用网之间的隧道生成的准备。READY 消

息可以包括诸如L2TP这样的使用中的VPN协议，本地网A（200A）的网络地址10.0.0.0/24，专用网B（200B）的网络地址10.0.0.0/24，将在VPN隧道中用于专用网A（200A）的网络地址10.0.1.0/24，以及将在VPN隧道中用于专用网B（200B）的网络地址10.0.2.0/24。

当网关A（100A）接收READY消息时，网关A（100A）根据将被使用的VPN协议设置VPN处理器146B为网关B（100B）的VPN客户机。当HTIP处理器146A`驱动VPN客户机时，在网关A（100A）和网关B（100B）之间生成VPN（L2TP）隧道。

根据上述方法，在网关A（100A）和网关B（100B）之间生成VPN隧道，以及被传送到网关A（100A）的VPN隧道的末端的数据分组被传送到网关B（100B）的VPN隧道的末端。

当完成VPN隧道的生成和链接时，以及在PPP连接之后，网关A（100A）参考专用网连接管理表132，在朝着网关A（100A）的VPN隧道处设置NAT。由于NAT被设置，所以当数据分组从专用网A（200A）通过网关A（100A）被传送到VPN隧道时，源地址10.0.0.X被变换为10.0.1.X。当数据分组从VPN隧道通过网关A（100A）被传送到专用网A时，目的地地址10.0.1.y被变换为10.0.0.y。网关B同样在朝着网关B（100B）的方向的VPN隧道上设置NAT。

图12示出了一个信号流程图，其解释了通过一个隧道在主机A（210A）和主机B（210B）之间的数据分组传送的过程，该隧道在专用网A和专用网B之间通过图11所示的方法而建立。

首先，专用网A（200A）的用户知道主机B（210B）的域名。当安装在主机A（210A）中的应用程序214将一个DNS询问发送到网关A（100A）时，询问对应于主机B（210B）域名的IP地址，网关A（100A）的DNS处理器143查询该专用网连接管理表132。如果存在专用网A（200A）和专用网B（200B）之间建立的VPN隧道，则当识别了NAT被要求用于通过隧道的数据分组传送时，询问将被用于主机B（210B）的VPN隧道的专用IP地址的DNS询问被发送到网关B（100B）。

当网关B（100B）的DSN处理器143`接收有关主机B（210B）的询问时，该DSN处理器143`发送一个IP地址10.0.2.5，该IP地址将在主机B（210B）的VPN隧道中作为对网关A（100A）的响应消息而被使用，以及网关A（100A）

重新发送该响应消息给主机A（210A）。为了简明，在附图中忽略了发送DNS询问和响应该询问的过程。之后，主机A（210A）传送一个数据分组给网关A（100A），以便发送该数据分组到主机B（210B）。地址10.0.2.5作为数据分组的目的地地址被写入，而地址10.0.0.4作为源地址被写入。

当网关A（100A）从主机A（210A）接收一个目的地是主机B（210B）的数据分组时，网关A（100A）参考路由表和转发设置，将该数据分组传送到网关A（100A）的隧道的末端。因为NAT在网关A（100A）的VPN隧道的末端处被设置，源地址10.0.0.4被变换为10.0.1.4，以及具有已变换源地址的数据分组被传送到网关B（100B）的隧道末端。

当源地址通过NAT被变换，从而该具有已变换源地址的数据分组被传送到网关B（100B）的末端时，网关B（100B）通过在VPN隧道的末端中设置的NAT将目的地地址10.0.2.5变换成10.0.0.5。在目的地地址通过NAT被转换之后，参考路由表和转发设置，将具有已变换目的地地址的数据分组传送到主机B（210B）。

主机B（210B）发送一个响应到主机A（210A），因此，随着重复数据分组传送过程来执行通信。

图13示出一个信号流程图，其解释了在两个专用网A和B之间形成VPN隧道的过程，其中专用网A的扩展网络ID被包括在专用网B的扩展网络ID中。

首先，专用网A（200A）的用户通过Web浏览器212在主机A（210A）处读取隧道建立请求页，其由网关A（100A）的Web服务器147来提供。因此，为了响应隧道建立的用户请求，网关A（100A）通过DNS处理器143从位于因特网中的DNS服务器330获取一个网关B（100B）的公共IP地址211.32.119.136。为了简明，在附图中忽略了发送DNS询问和响应该询问的过程。

当网关A（100A）获得网关B（100B）的公共IP地址时，HTIP处理器146A驱动HTIP程序，以及网关B（100B）请求网关B（100B）的HTIP处理器146A`在专用网之间生成隧道。该隧道建立请求消息可以包括诸如L2TP这样的将被使用的VPN协议，专用网A（200A）的网络地址10.0.0.0/24，以及在VPN隧道中用于代替专用网A（200A）的网络地址的网络地址（10.0.0.0/24，10.0.1.0/24，10.0.2.0/24，...）。

网关 B（100B）的 HTIP 处理器（146A`）从网关 A（100A）接收隧道建立请求消息，并分析该已接收的消息。因为在 VPN 隧道中用于代替专用网 A（200A）的网络地址的网络地址（10.0.0.0/24，10.0.1.0/24，...）被包括在专用网 B（200B）的网络地址中，所以网关 B（100B）的 HTIP 处理器 146A′发送一个 NAK 消息到网关 A(100A)。该 NAK 消息可以包括从网关 A(100A)到网关 B（100B）的用于重协商的隧道建立请求消息的一部分，诸如在 VPN 隧道中将被用于替代专用网 A（200A）的网络地址的网络地址，以及专用网 B（200B）的网络地址 10.0.0.0/16。

当网关 A（100A）的 HTIP 处理器 146A 从网关 B（100B）接收 NAK 消息时，HTIP 处理器 146 分析 NAK 消息的内容，同时重新发送一个隧道建立请求。第二个隧道建立请求消息可以包括诸如 L2TP 这样的将被使用的 VPN 协议，专用网 A（200A）的网络地址 10.0.0.0/24，以及在 VPN 隧道中用于替代专用网 A（200A）的网络地址的网络地址（10.2.0.0/24，10.2.1.0/24，...）。

当从网关 A（100A）接收到该隧道建立请求消息时，网关 B（100B）的 HTIP 处理器 146A′分析所接收的请求，以及如果确定其合适，则发送一个响应消息给该请求。该响应消息可以包括将被使用的诸如 L2TP 这样的 VPN 协议，专用网 B（200B）的网络地址 10.0.0.0/16，在 VPN 隧道中将用于替代专用网 B（200B）的网络地址的网络地址（10.1.0.0/16，10.2.0.0/16，...），专用网 A（200A）的网络地址 10.0.0.0/24，以及将在 VPN 隧道中用于替代专用网 A（200A）的网络地址的网络地址 10.2.0.0/24。

当从网关 B（100B）接收到一个响应消息时，网关 A（100A）的 HTIP 处理器 146A 分析已接收的消息并且如果确定其合适，则发送 ACK 消息给网关 B(100B)。该 ACK 消息可以包括将被使用的诸如 L2TP 这样的 VPN 协议，专用网 A（200A）的网络地址 10.0.0.0/24，在 VPN 隧道中将用于替代专用网 A（100A）的网络地址的网络地址 10.2.0.0/24，专用网 B（200B）的网络地址 10.0.0.0/16，以及将在 VPN 隧道中代替专用网 B（200B）的网络地址的网络地址 10.1.0.0/16。因为将在 VPN 隧道中使用的用于代替专用网 A（200A）的网络地址的网络地址是不同的，所以认识到网关 A（100A）需要 NAT。

在发送和接收 ACK 消息之后，在网关 A（100A）和网关 B（100B）处生成专用网连接管理表 132 和 132′。由网关 A（100A）产生的表可以包括使用中的诸如 L2TP 这样的 VPN 协议，在专用网之间的隧道的 ID，网关 B(100B)

的域名，表明网关 B（100B）是 VPN 服务器的一个项目，网关 A（200A）的网络地址 10.0.0.0/24，以及专用网 B（200B）的网络地址 10.0.0.0/16，将在 VPN 隧道中代替专用网 A（200A）的网络地址的网络地址 10.2.0.0/24，以及将在 VPN 隧道中用于代替专用网 B（200B）的网络地址的网络地址 10.1.0.0/16。

当网关 B（100B）接收 ACK 消息时，网关 B（100B）将 VPN 处理器 146B′设置成 VPN 服务器，以便根据将被使用的 VPN 协议生成 VPN 隧道。当完成准备在专用网之间的隧道建立时，该准备包括将 VPN 处理器 146B′设置为 VPN 服务器，网关 B（100B）的 HTIP 处理器 146A′发送 READY 消息到网关 A（100A），相应地通知已经完成在专用网之间建立隧道的准备。READY 消息可以包括使用中的诸如 L2TP 这样的 VPN 协议，专用网 A（200A）的网络地址 10.0.0.0/24，专用网 B（200B）的网络地址 10.0.0.0/16，在 VPN 隧道中用于专用网 A（200A）的网络地址 10.2.0.0/24，以及在 VPN 隧道中用于专用网 B（200B）的网络地址 10.1.0.0/16。

当接收了 READY 消息时，网关 A（100A）的 HTIP 处理器 146A 根据将被使用的 VPN 协议将 VPN 处理器 146B 设置为网关 B（100B）的 VPN 客户机。当 HTIP 处理器 146A 驱动 VPN 客户机时，在网关 A（100A）和网关 B（100B）之间生成 VPN（L2TP）隧道。

如上所述，VPN 隧道在网关 A（100A）和网关 B（100B）之间被生成。被传送到网关 A（100A）的 VPN 隧道的末端的数据分组被传送到网关 B（100B）的 VPN 隧道的末端。

当 VPN 隧道被生成并连接时，参考专用网连接管理表 132，网关 A（100A）的 HTIP 处理器 146A 在朝着网关 A（100A）的 VPN 隧道处设置 NAT。当 NAT 被设置后，从专用网 A（200A）通过网关 A（100A）将数据分组传送到 VPN 隧道时，源地址 10.0.0.x 被变换成 10.2.0.x。当数据分组通过 VPN 隧道和网关 A（100A）被传送到专用网 A（200A）时，目的地地址 10.2.0.y 被变换成 10.0.0.y。同样的，网关 B（100B）的 HTIP 处理器 146A′在朝着网关 B（100B）的 VPN 隧道处设置 NAT。

因为 NAT 在网关 A（100A）和网关 B（100B）之间的 VPN 隧道的两端被设置，所以通过图 12 所示的数据分组的传送，主机 A（210A）和主机 B（210B）能够进行相互通信。

根据参考本发明的一个实施例所述的网关，用户使用网络的范围被大大的扩展了，因为其能够连接专用网和公共网络，或者在专用网之间进行连接。因此，增加了用户的便利性，而且通过多种通信，本地网络的用户能够更加有效地与其它本地网络的用户通信。因此，在本地网络中的信息或者设备被更加积极地共享。此外，在当前的 IPv4 环境下能够解决公共 IP 地址的短缺的问题，因此，网络的整体性能改善了。

如上所述参考本发明第二个实施例的方法被称为“本地对本地隧道启动”协议（HTIP）。根据该 HTIP，请求在专用网之间生成 VPN 隧道的信息能够被提前交换和协商，因此，能够最小化 VPN 隧道建立的提前设置的请求。同样，通过使用在 VPN 处理器和 NAT/NAPT 处理器的控制中的 HTIP 处理器的已协商信息，已有的诸如 PPTP 或 L2TP 这样的 VPN 协议能够被直接使用而不需要任何的修改。根据 HTLP，提前做出协商，因此最新形成的 VPN 隧道的网络地址与已有的 VPN 隧道的网络地址不相互冲突。结果，能够在两个或多个专用网中建立交叉的 VPN 隧道。

上述的实施例和优点仅是示范性的，而不认为限制本发明。本发明能够容易地用于其它类型的设备。同样，本发明实施例的描述是示例性的，而没有限制权利要求的范围，并且对本领域的普遍技术人员来说多种替代，修改是清楚明了的。

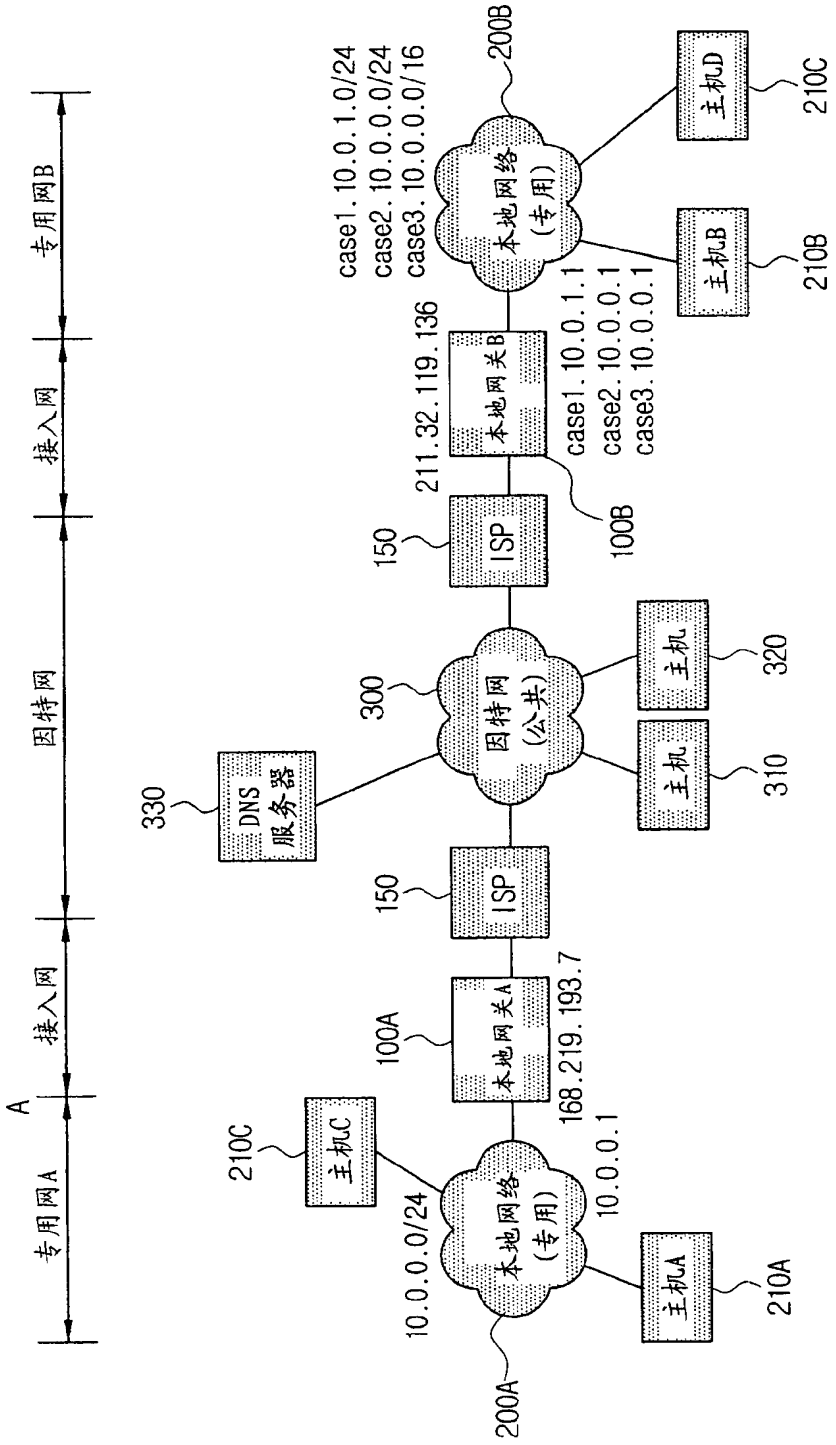

专用网A
接入网
A
因特网
接入网
专用网B
主机C
210C
10.0.0.0/24
本地网络
(专用)
200A
本地网关A
100A
168.219.193.7
10.0.0.1
主机A
210A
ISP
150
ISP
150
DNS
服务器
330
因特网
(公共)
300
主机
310
主机
320
211.32.119.136
本地网关B
100B
case1. 10.0.1.1
case2. 10.0.0.1
case3. 10.0.0.1
case1. 10.0.1.0/24
case2. 10.0.0.0/24
case3. 10.0.0.0/16
本地网络
(专用)
200B
主机B
210B
主机D
210C

图 1

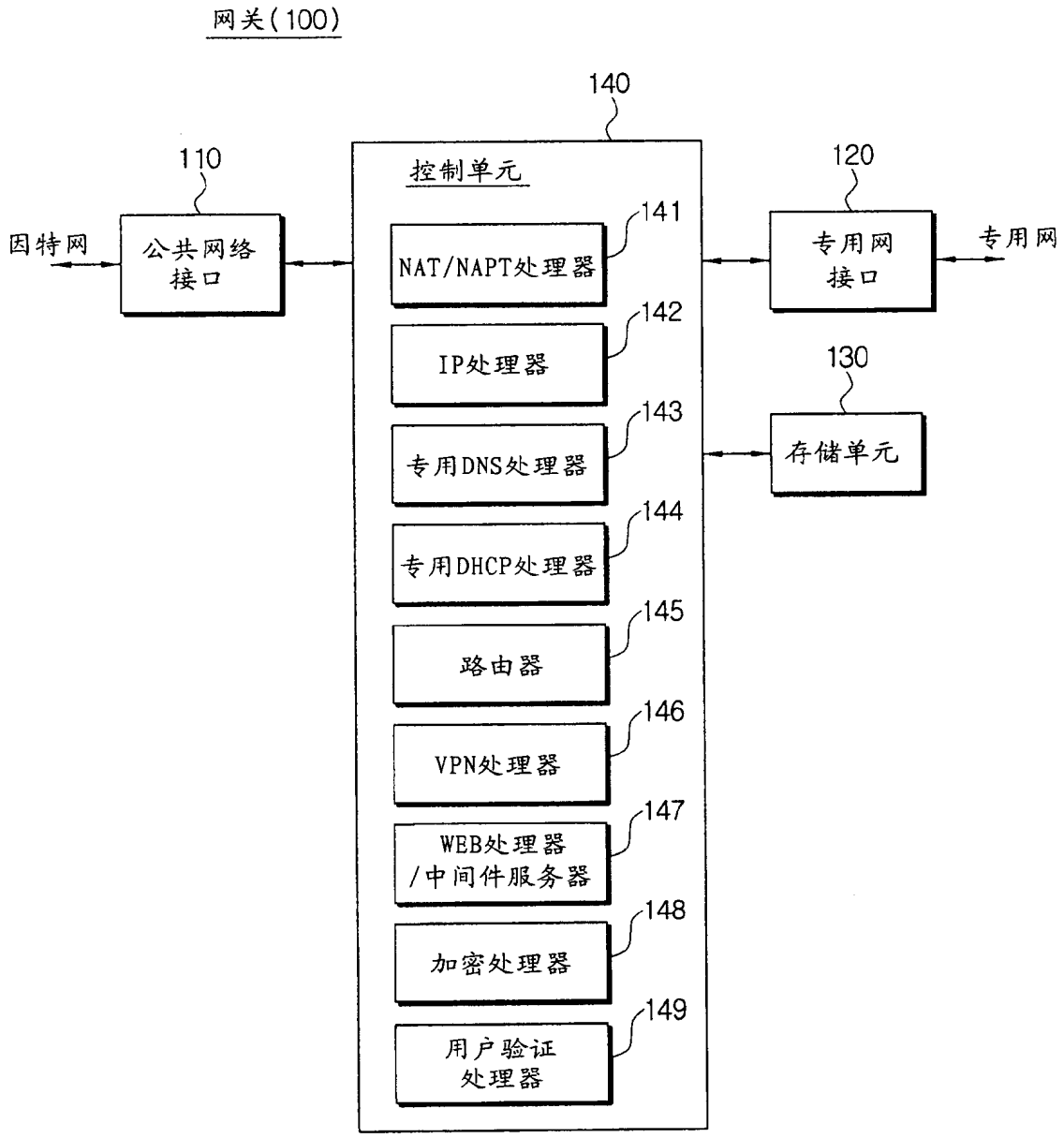

网关(100)
140
控制单元
110
因特网
公共网络接口
141
NAT/NAPT处理器
142
IP处理器
143
专用DNS处理器
144
专用DHCP处理器
145
路由器
146
VPN处理器
147
WEB处理器/中间件服务器
148
加密处理器
149
用户验证处理器
120
专用网接口
专用网
130
存储单元

图 2

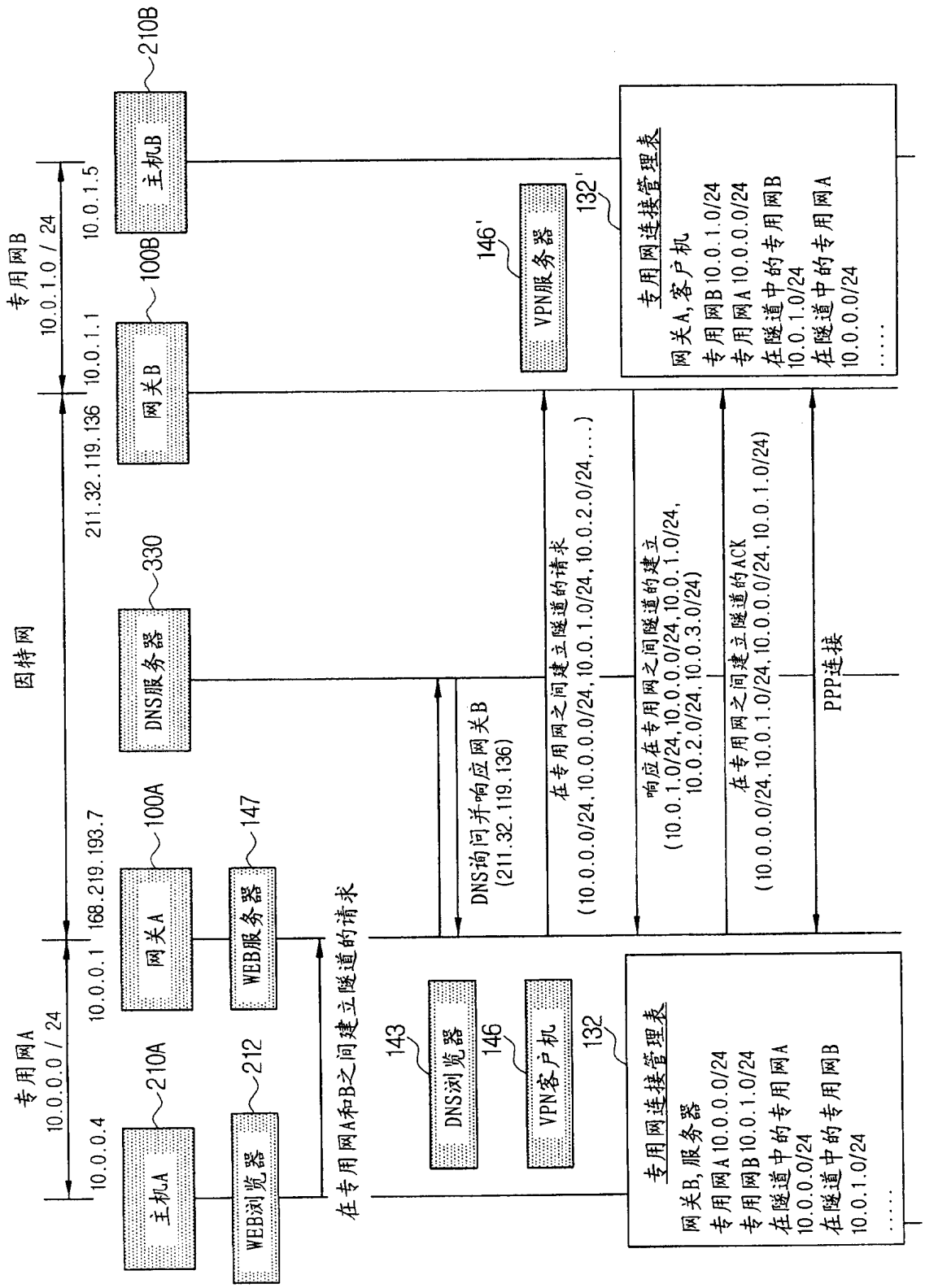

专用网A
10.0.0.0 / 24
10.0.0.4
主机A
210A
WEB浏览器
212
10.0.0.1
168.219.193.7
网关A
100A
WEB服务器
147
因特网
211.32.119.136
DNS服务器
330
10.0.1.1
网关B
100B
10.0.1.5
主机B
210B
专用网B
10.0.1.0 / 24
在专用网A和B之间建立隧道的请求
143
DNS浏览器
146
VPN客户机
132
专用网连接管理表
网关B,服务器
专用网A 10.0.0.0/24
专用网B 10.0.1.0/24
在隧道中的专用网A
10.0.0.0/24
在隧道中的专用网B
10.0.1.0/24
.....
DNS询问并响应网关B
(211.32.119.136)
在专用网之间建立隧道的请求
(10.0.0.0/24,10.0.0.0/24,10.0.1.0/24,10.0.2.0/24,...)
响应在专用网之间隧道的建立
(10.0.1.0/24,10.0.0.0/24,10.0.1.0/24,
10.0.2.0/24,10.0.3.0/24)
在专用网之间建立隧道的ACK
(10.0.0.0/24,10.0.1.0/24,10.0.0.0/24,10.0.1.0/24)
PPP连接
146'
VPN服务器
132'
专用网连接管理表
网关A,客户机
专用网B 10.0.1.0/24
专用网A 10.0.0.0/24
在隧道中的专用网B
10.0.1.0/24
在隧道中的专用网A
10.0.0.0/24
.....

图 3

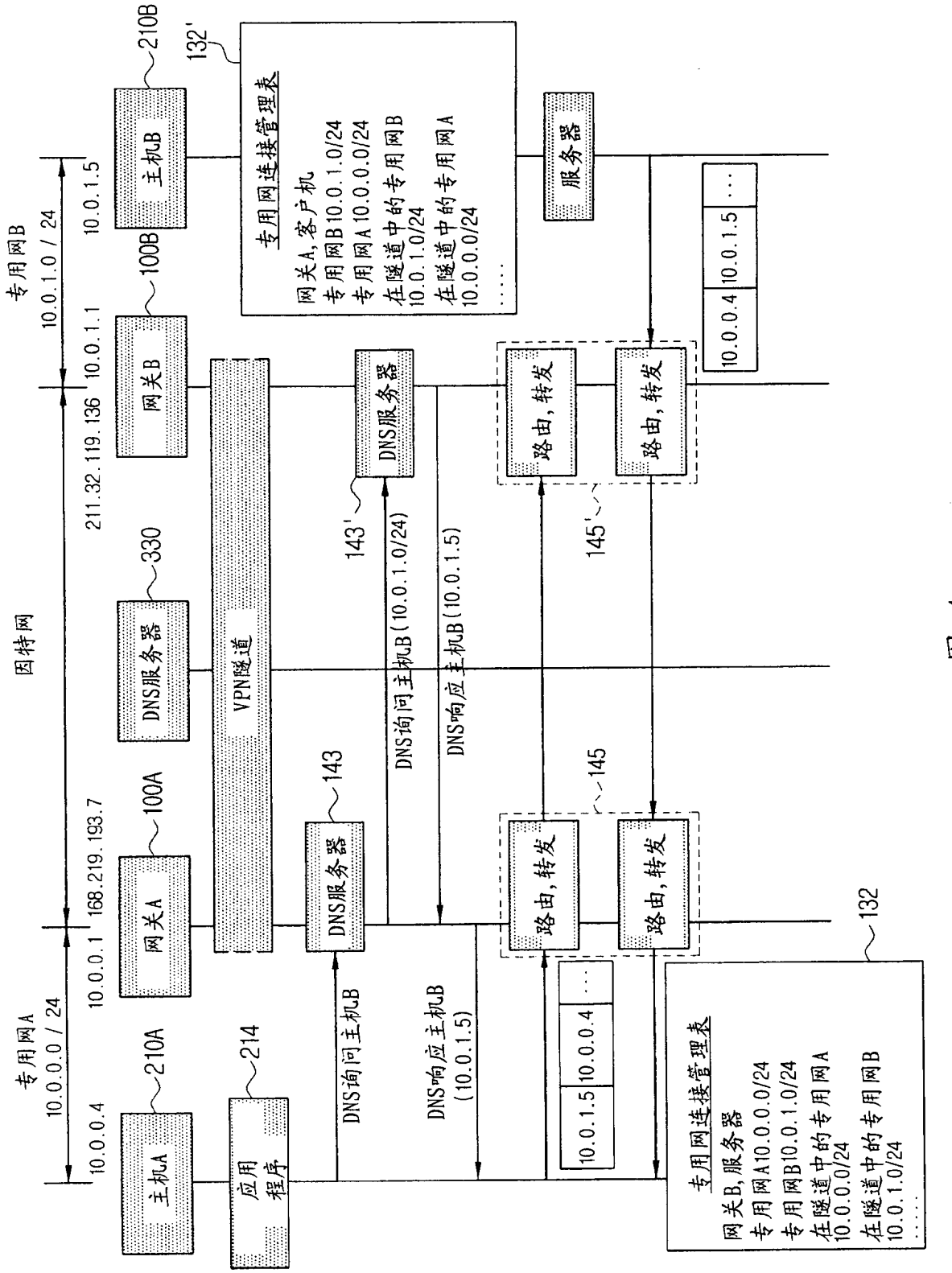

专用网A
10.0.0.0 / 24
10.0.0.4
主机A
210A
应用程序
214
10.0.0.1
168.219.193.7
网关A
100A
因特网
211.32.119.136
DNS服务器
330
VPN隧道
DNS服务器
143
DNS询问主机B
DNS响应主机B
(10.0.1.5)
DNS询问主机B(10.0.1.0/24)
DNS响应主机B(10.0.1.5)
143'
DNS服务器
路由,转发
145
145'
路由,转发
路由,转发
10.0.1.5
10.0.0.4
专用网连接管理表
网关B,服务器
专用网A10.0.0.0/24
专用网B10.0.1.0/24
在隧道中的专用网A
10.0.0.0/24
在隧道中的专用网B
10.0.1.0/24
132
专用网B
10.0.1.0 / 24
10.0.1.1
网关B
100B
10.0.1.5
主机B
210B
132'
专用网连接管理表
网关A,客户机
专用网B10.0.1.0/24
专用网A10.0.0.0/24
在隧道中的专用网B
10.0.1.0/24
在隧道中的专用网A
10.0.0.0/24
服务器
10.0.0.4
10.0.1.5

图 4

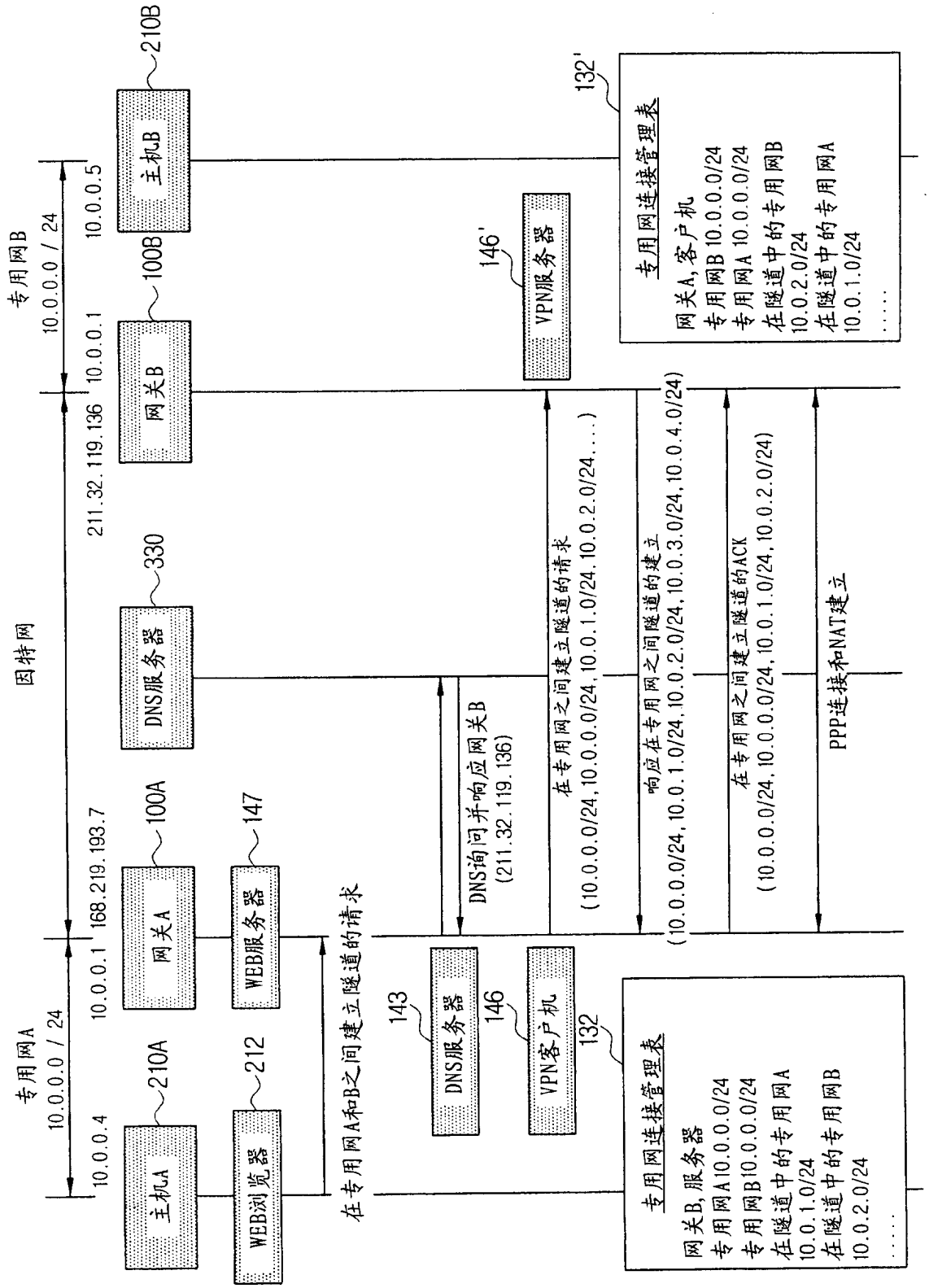

专用网A
10.0.0.0 / 24
10.0.0.4
主机A
210A
WEB浏览器
212
10.0.0.1
168.219.193.7
网关A
100A
WEB服务器
147
在专用网A和B之间建立隧道的请求
因特网
211.32.119.136
DNS服务器
330
DNS询问并响应网关B
(211.32.119.136)
143
DNS服务器
146
VPN客户机
132
专用网连接管理表
网关B,服务器
专用网A10.0.0.0/24
专用网B10.0.0.0/24
在隧道中的专用网A
10.0.1.0/24
在隧道中的专用网B
10.0.2.0/24
.....
专用网B
10.0.0.0 / 24
10.0.0.1
网关B
100B
10.0.0.5
主机B
210B
在专用网之间建立隧道的请求
(10.0.0.0/24,10.0.0.0/24,10.0.1.0/24,10.0.2.0/24,....)
146'
VPN服务器
响应在专用网之间隧道的建立
(10.0.0.0/24,10.0.1.0/24,10.0.2.0/24,10.0.3.0/24,10.0.4.0/24)
在专用网之间建立隧道的ACK
(10.0.0.0/24,10.0.0.0/24,10.0.1.0/24,10.0.2.0/24)
PPP连接和NAT建立
132'
专用网连接管理表
网关A,客户机
专用网B 10.0.0.0/24
专用网A 10.0.0.0/24
在隧道中的专用网B
10.0.2.0/24
在隧道中的专用网A
10.0.1.0/24
.....

图 5

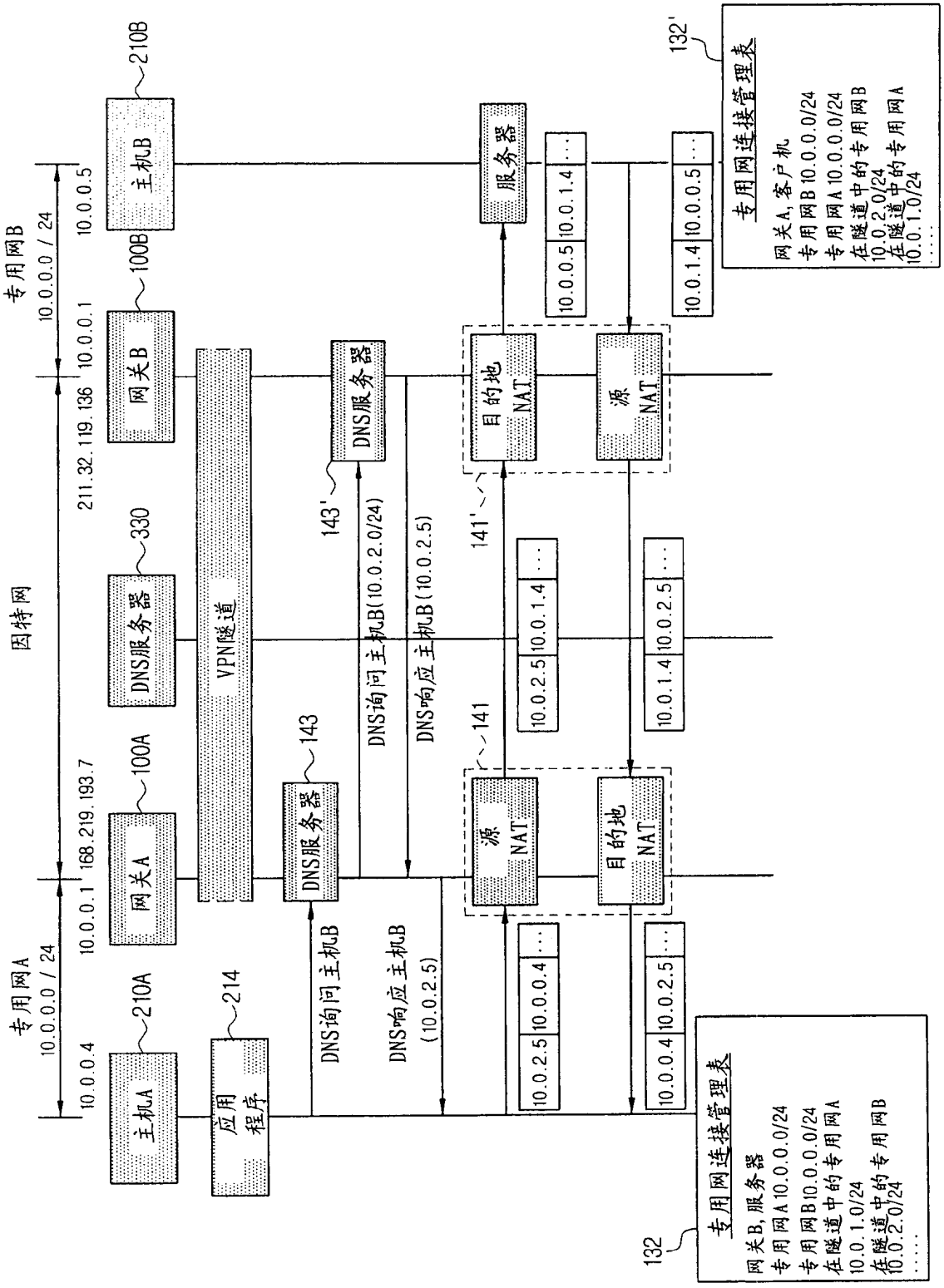

专用网A
10.0.0.0 / 24
10.0.0.4
主机A
210A
应用程序
214
10.0.0.1
168.219.193.7
网关A
100A
因特网
DNS服务器
330
VPN隧道
DNS服务器
143
DNS询问主机B
DNS响应主机B
(10.0.2.5)
DNS询问主机B(10.0.2.0/24)
DNS响应主机B(10.0.2.5)
143'
211.32.119.136
10.0.0.1
网关B
100B
专用网B
10.0.0.0 / 24
10.0.0.5
主机B
210B
141
源 NAT
10.0.2.5
10.0.0.4
目的地 NAT
10.0.0.4
10.0.2.5
141'
目的地 NAT
10.0.2.5
10.0.1.4
源 NAT
10.0.1.4
10.0.0.5
服务器
10.0.0.5
10.0.1.4
132
专用网连接管理表
网关B, 服务器
专用网A 10.0.0.0/24
专用网B 10.0.0.0/24
在隧道中的专用网A
10.0.1.0/24
在隧道中的专用网B
10.0.2.0/24
.....
132'
专用网连接管理表
网关A, 客户机
专用网B 10.0.0.0/24
专用网A 10.0.0.0/24
在隧道中的专用网B
10.0.2.0/24
在隧道中的专用网A
10.0.1.0/24
.....

图 6

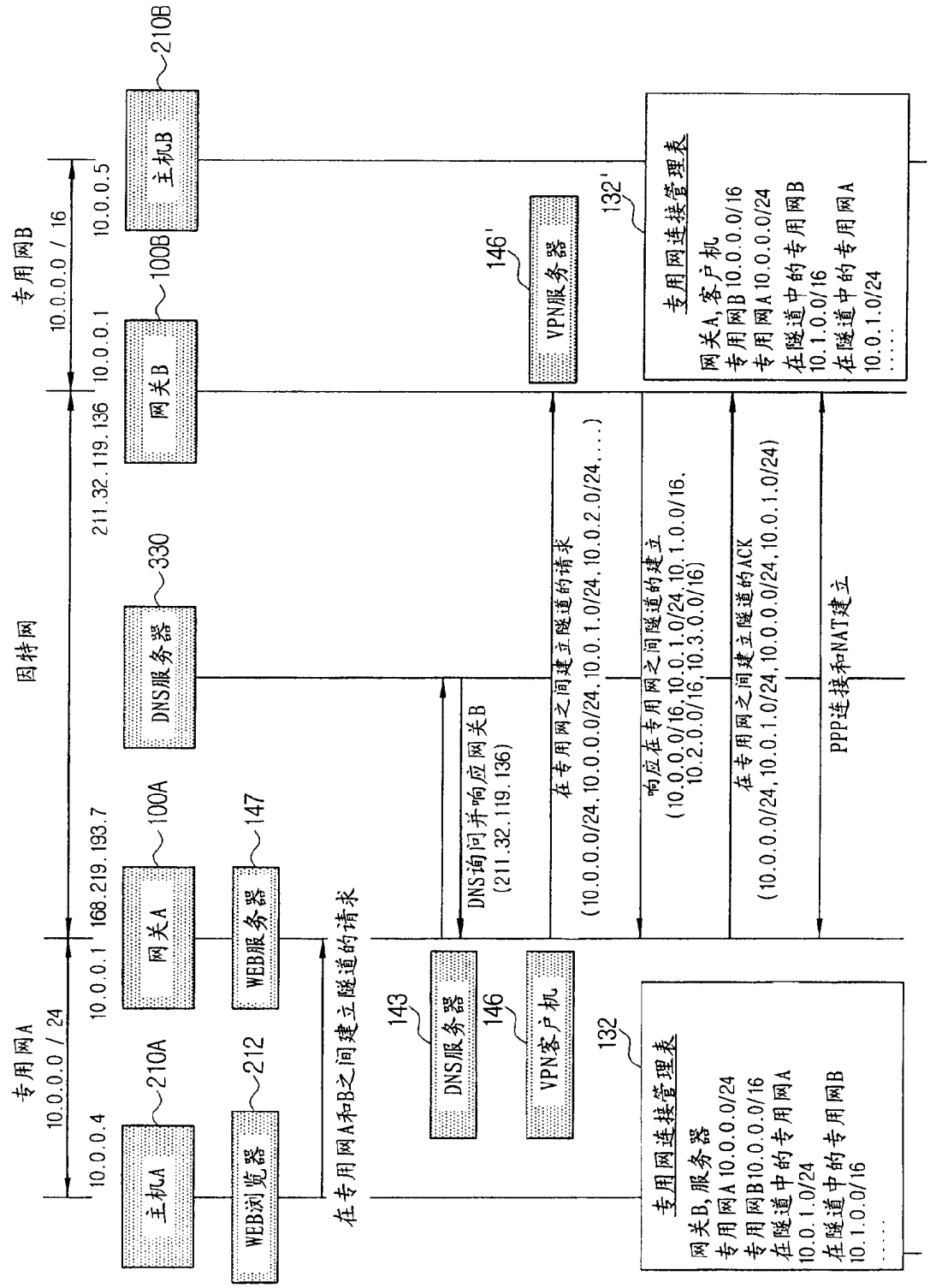

专用网A
10.0.0.0 / 24
10.0.0.4
主机A
210A
WEB浏览器
212
10.0.0.1
网关A
100A
168.219.193.7
WEB服务器
147
在专用网A和B之间建立隧道的请求
因特网
211.32.119.136
DNS服务器
330
专用网B
10.0.0.0 / 16
10.0.0.1
网关B
100B
10.0.0.5
主机B
210B
143
DNS服务器
DNS询问并响应网关B
(211.32.119.136)
146
VPN客户机
在专用网之间建立隧道的请求
(10.0.0.0/24,10.0.0.0/24,10.0.1.0/24,10.0.2.0/24,....)
146'
VPN服务器
132
专用网连接管理表
网关B,服务器
专用网A 10.0.0.0/24
专用网B10.0.0.0/16
在隧道中的专用网A
10.0.1.0/24
在隧道中的专用网B
10.1.0.0/16
.....
响应在专用网之间隧道的建立
(10.0.0.0/16,10.0.1.0/24,10.1.0.0/16,
10.2.0.0/16,10.3.0.0/16)
在专用网之间建立隧道的ACK
(10.0.0.0/24,10.0.1.0/24,10.0.0.0/24,10.0.1.0/24)
PPP连接和NAT建立
132'
专用网连接管理表
网关A,客户机
专用网B 10.0.0.0/16
专用网A 10.0.0.0/24
在隧道中的专用网B
10.1.0.0/16
在隧道中的专用网A
10.0.1.0/24
.....

图 7

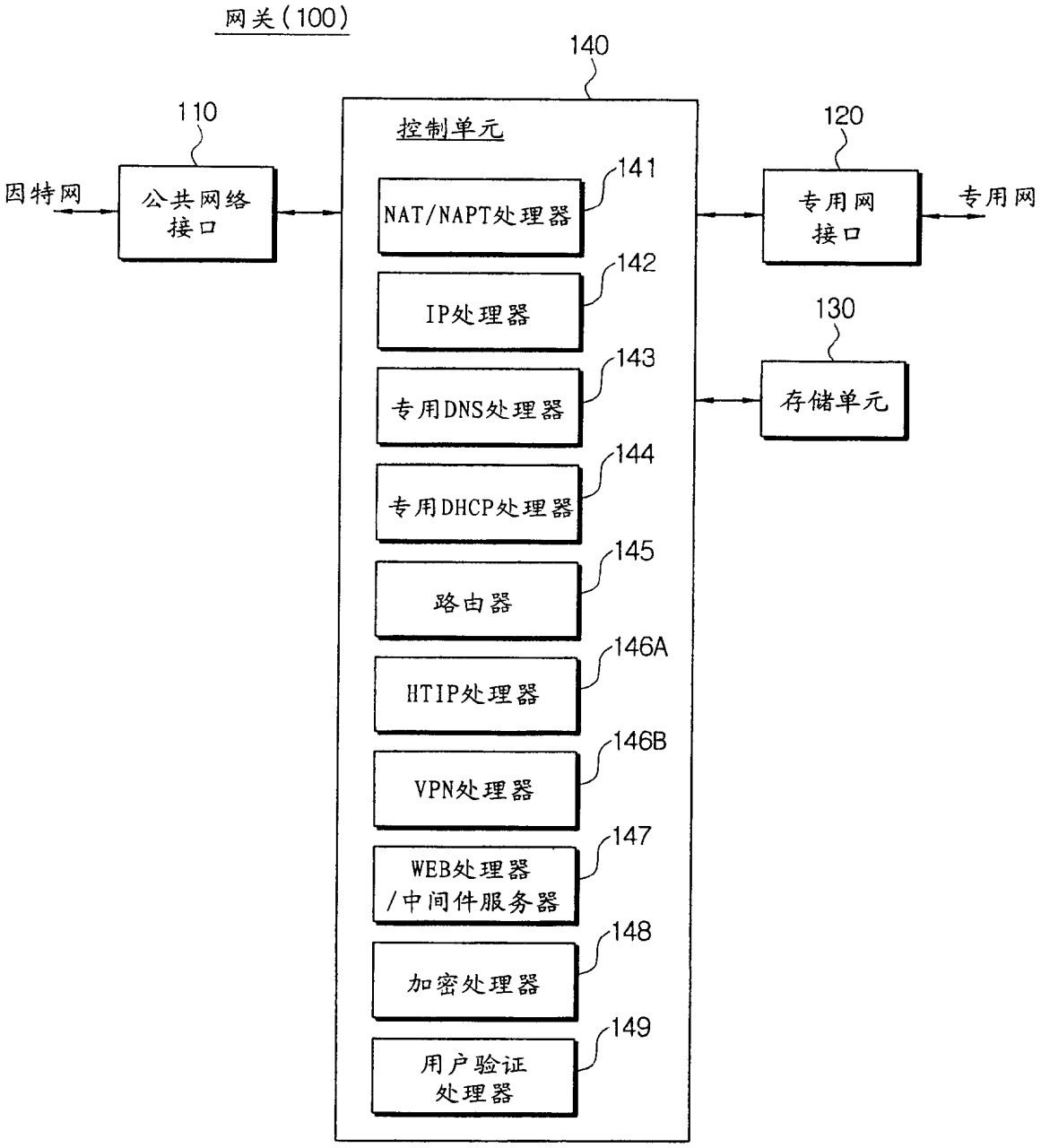

网关(100)
140
控制单元
110
因特网
公共网络接口
141
NAT/NAPT处理器
142
IP处理器
143
专用DNS处理器
144
专用DHCP处理器
145
路由器
146A
HTIP处理器
146B
VPN处理器
147
WEB处理器/中间件服务器
148
加密处理器
149
用户验证处理器
120
专用网接口
专用网
130
存储单元

图 8

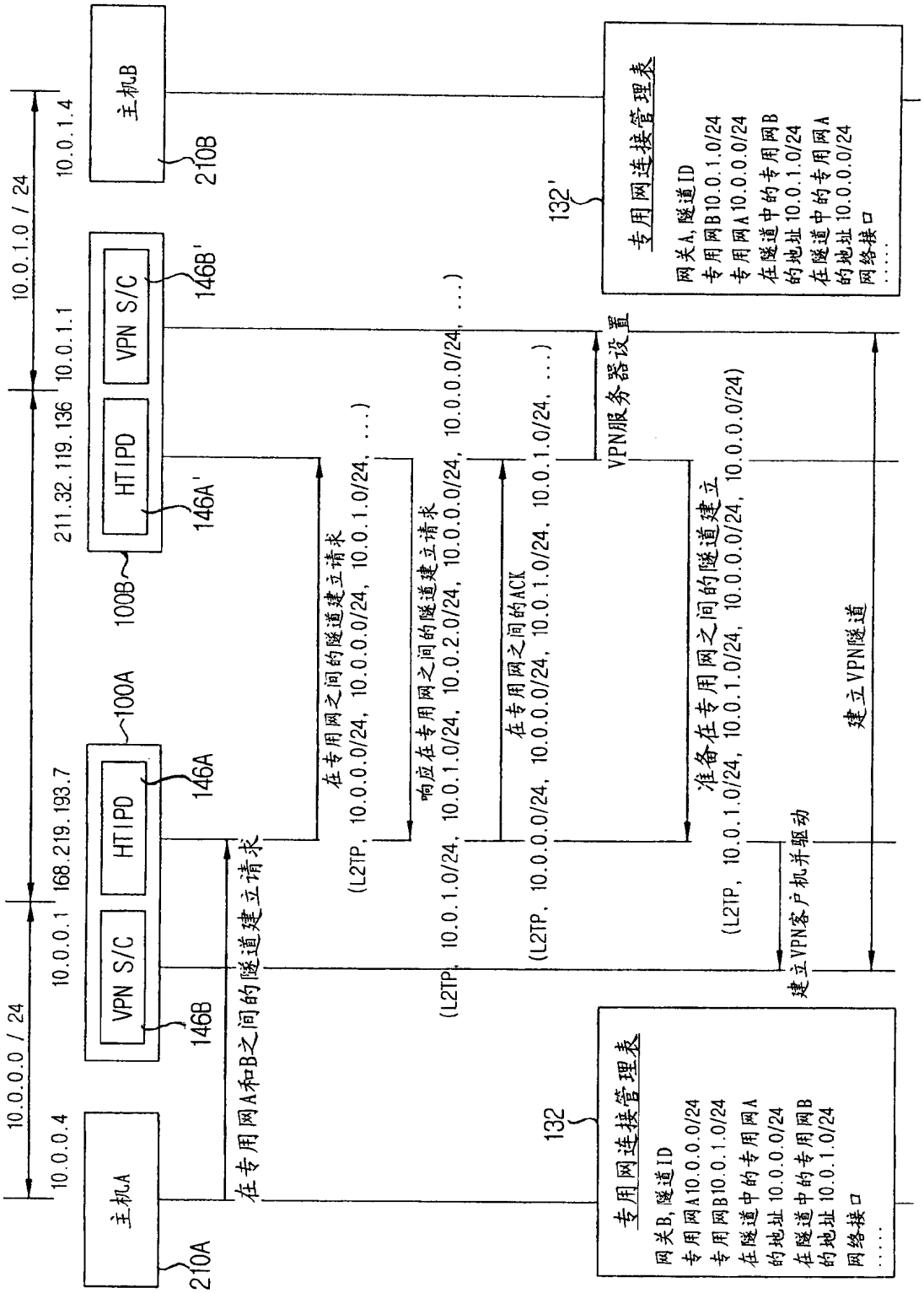

专用网A
网关A
因特网
网关B
专用网B
10.0.0.0 / 24
10.0.0.4
主机A
210A
10.0.0.1
168.219.193.7
VPN S/C
HTIPD
100A
146B
146A
在专用网A和B之间的隧道建立请求
211.32.119.136
10.0.1.1
10.0.1.0 / 24
10.0.1.4
主机B
210B
HTIPD
VPN S/C
100B
146A'
146B'
在专用网之间的隧道建立请求
(L2TP, 10.0.0.0/24, 10.0.0.0/24, 10.0.1.0/24, ...)
响应在专用网之间的隧道建立请求
(L2TP, 10.0.1.0/24, 10.0.2.0/24, 10.0.0.0/24, 10.0.0.0/24, ...)
在专用网之间的ACK
(L2TP, 10.0.0.0/24, 10.0.0.0/24, 10.0.1.0/24, 10.0.1.0/24, ...)
VPN服务器设置
准备在专用网之间的隧道建立
(L2TP, 10.0.1.0/24, 10.0.1.0/24, 10.0.0.0/24, 10.0.0.0/24)
建立VPN客户机并驱动
建立VPN隧道
132
专用网连接管理表
网关B,隧道ID
专用网A10.0.0.0/24
专用网B10.0.1.0/24
在隧道中的专用网A
的地址 10.0.0.0/24
在隧道中的专用网B
的地址 10.0.1.0/24
网络接口
.....
132'
专用网连接管理表
网关A,隧道ID
专用网B10.0.1.0/24
专用网A10.0.0.0/24
在隧道中的专用网B
的地址 10.0.1.0/24
在隧道中的专用网A
的地址 10.0.0.0/24
网络接口
.....

图 9

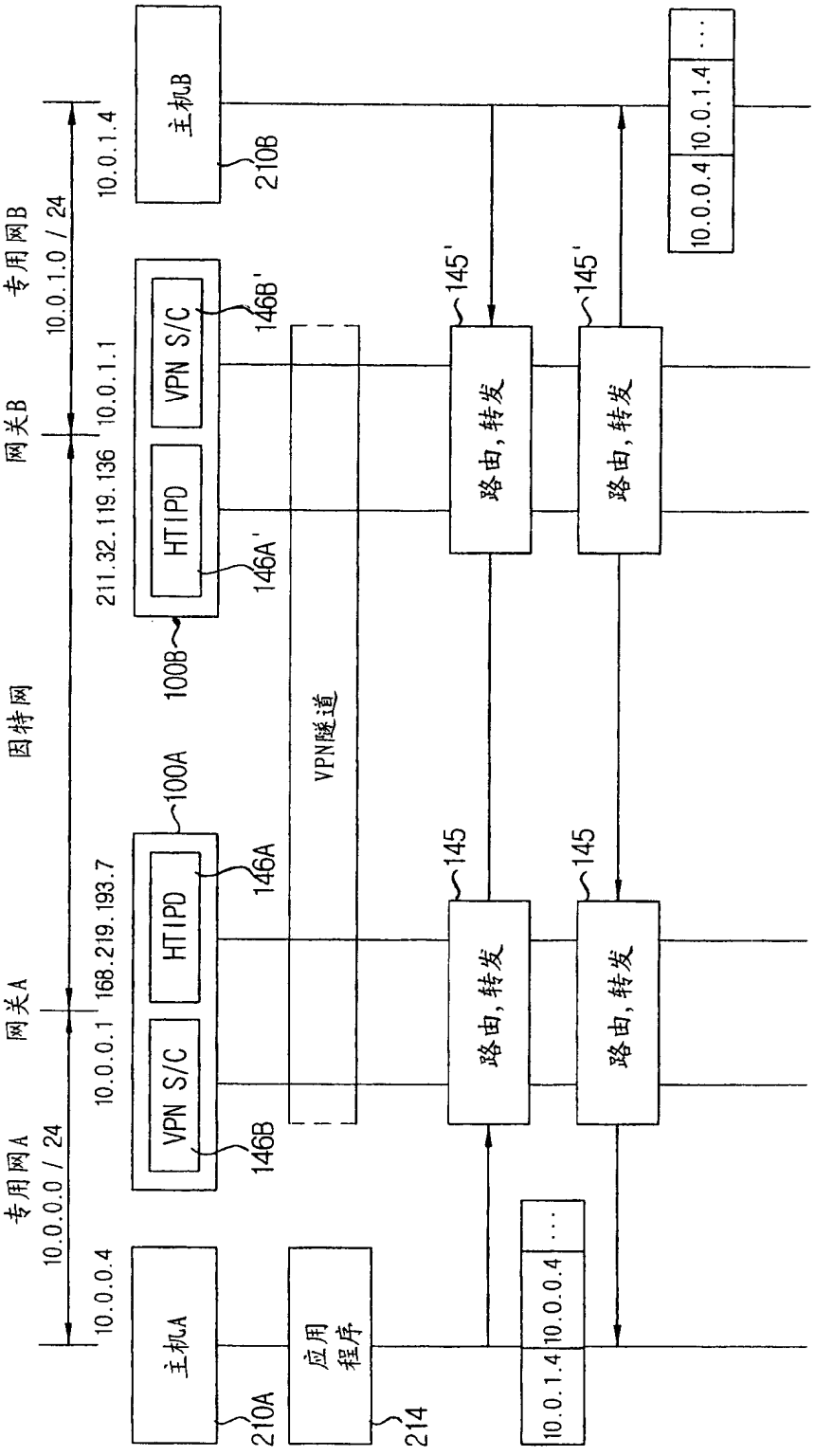

专用网A
10.0.0.0 / 24
10.0.0.4
主机A
210A
应用程序
214
10.0.0.1
网关A
168.219.193.7
VPN S/C
HTIPD
100A
146B
146A
因特网
VPN隧道
100B
211.32.119.136
HTIPD
VPN S/C
146A'
146B'
网关B
10.0.1.1
专用网B
10.0.1.0 / 24
10.0.1.4
主机B
210B
路由,转发
145
145'
10.0.1.4
10.0.0.4
...

图 10

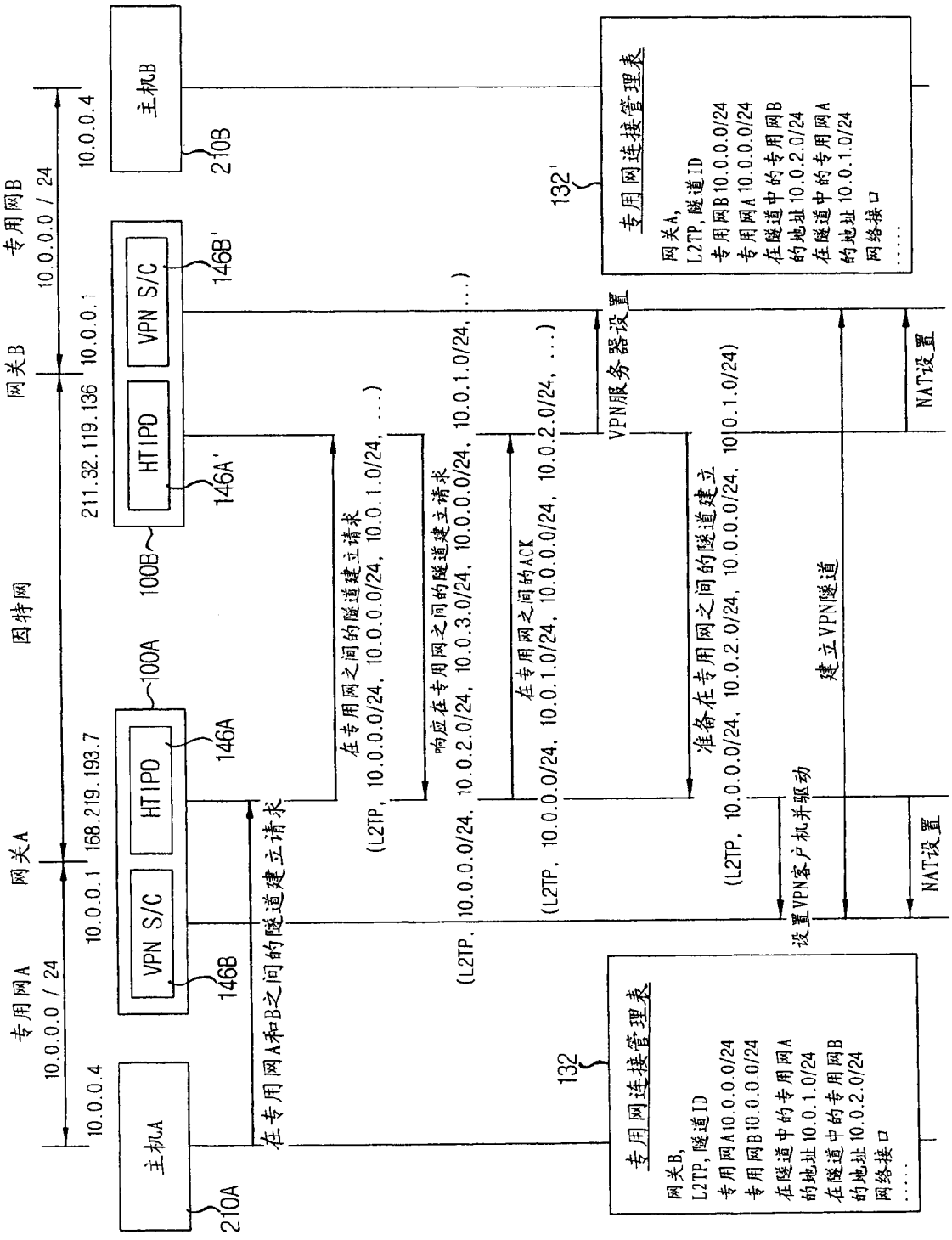

专用网A
10.0.0.0 / 24
10.0.0.4
主机A
210A
网关A
10.0.0.1
168.219.193.7
VPN S/C
HTIPD
100A
146B
146A
因特网
在专用网A和B之间的隧道建立请求
(L2TP, 10.0.0.0/24, 10.0.2.0/24, 10.0.3.0/24, ...)
在专用网之间的隧道建立请求
(L2TP, 10.0.0.0/24, 10.0.0.0/24, 10.0.1.0/24, ...)
响应在专用网之间的隧道建立请求
(L2TP, 10.0.0.0/24, 10.0.1.0/24, 10.0.0.0/24, 10.0.2.0/24, ...)
在专用网之间的ACK
网关B
211.32.119.136
10.0.0.1
100B
HTIPD
VPN S/C
146A'
146B'
专用网B
10.0.0.0 / 24
10.0.0.4
主机B
210B
132
专用网连接管理表
网关B,
L2TP,隧道ID
专用网A10.0.0.0/24
专用网B10.0.0.0/24
在隧道中的专用网A的地址10.0.1.0/24
在隧道中的专用网B的地址10.0.2.0/24
网络接口
.....
设置VPN客户机并驱动
(L2TP, 10.0.0.0/24, 10.0.2.0/24, 10.0.0.0/24, 10.0.1.0/24)
准备在专用网之间的隧道建立
建立VPN隧道
132'
专用网连接管理表
网关A,
L2TP,隧道ID
专用网B10.0.0.0/24
专用网A10.0.0.0/24
在隧道中的专用网B的地址10.0.2.0/24
在隧道中的专用网A的地址10.0.1.0/24
网络接口
.....
VPN服务器设置
NAT设置
NAT设置

图 11

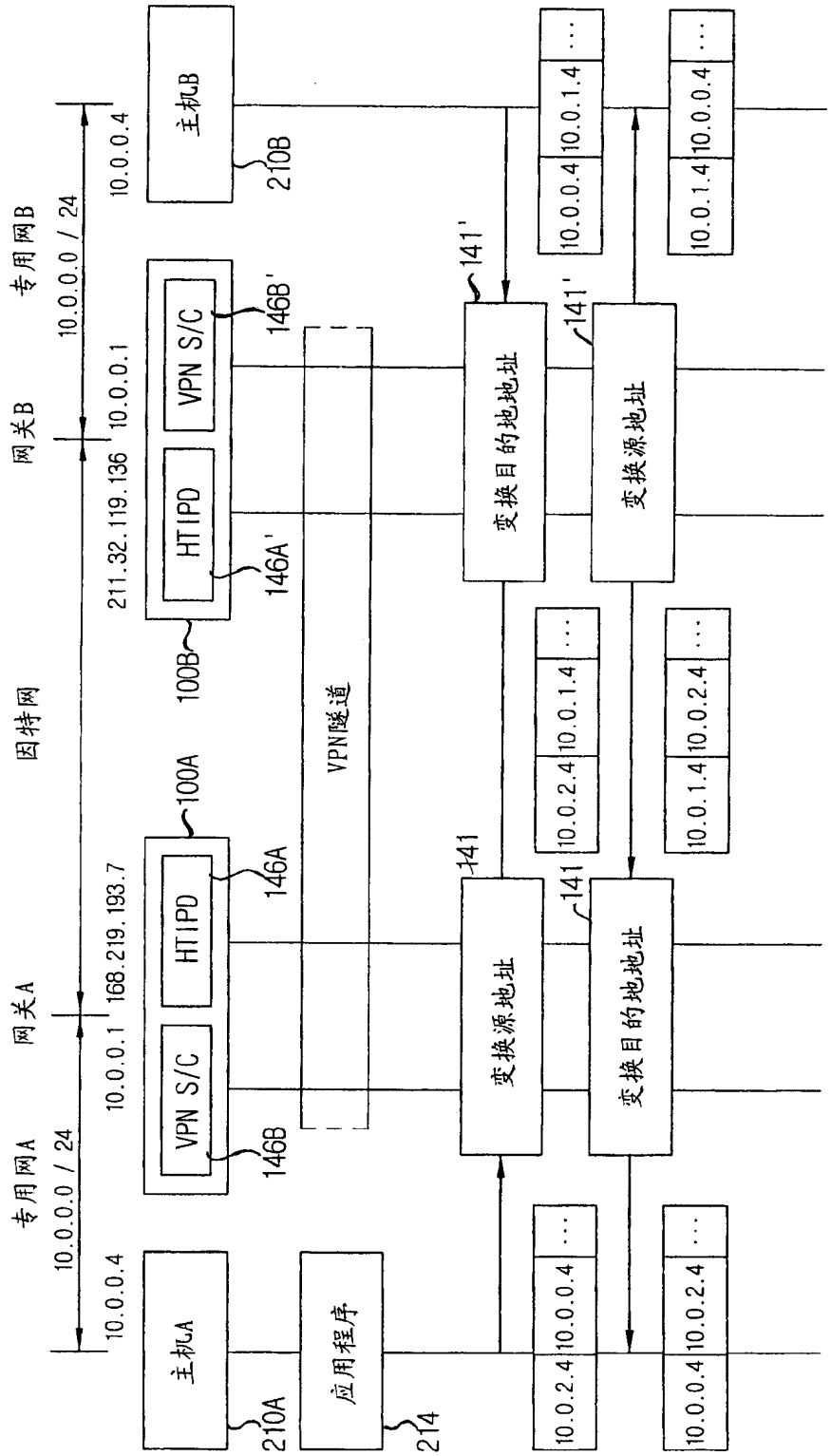

专用网A
10.0.0.0 / 24
网关A
因特网
网关B
专用网B
10.0.0.0 / 24
10.0.0.4
主机A
210A
应用程序
214
10.0.0.1
168.219.193.7
VPN S/C
HTIPD
100A
146B
146A
VPN隧道
211.32.119.136
10.0.0.1
HTIPD
VPN S/C
100B
146A'
146B'
10.0.0.4
主机B
210B
变换源地址
141
变换目的地地址
141
变换目的地地址
141'
变换源地址
141'
10.0.2.4
10.0.0.4
...
10.0.0.4
10.0.2.4
...
10.0.2.4
10.0.1.4
...
10.0.1.4
10.0.2.4
...
10.0.0.4
10.0.1.4
...
10.0.1.4
10.0.0.4
...

图 12

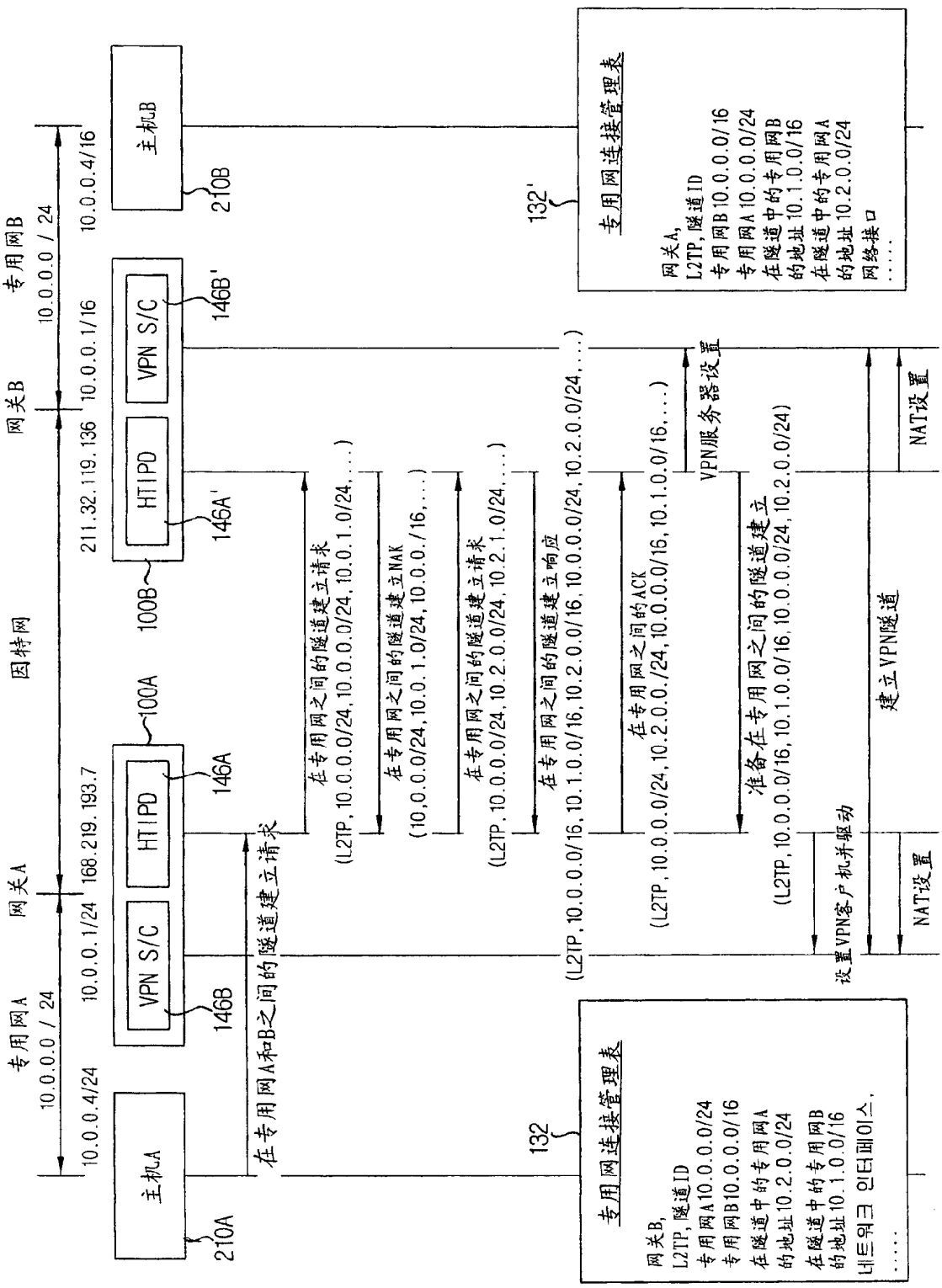

专用网A
10.0.0.0 / 24
网关A
因特网
网关B
专用网B
10.0.0.0 / 24
10.0.0.4/24
10.0.0.1/24
168.219.193.7
211.32.119.136
10.0.0.1/16
10.0.0.4/16
主机A
210A
VPN S/C
HTIPD
146B
100A
100B
HTIPD
VPN S/C
146A'
146B'
主机B
210B
在专用网A和B之间的隧道建立请求
在专用网之间的隧道建立请求
(L2TP, 10.0.0.0/24, 10.0.0.0/24, 10.0.1.0/24, ...)
在专用网之间的隧道建立NAK
(10,0.0.0/24,10.0.1.0/24,10.0.0./16,...)
在专用网之间的隧道建立请求
(L2TP, 10.0.0.0/24, 10.2.0.0/24, 10.2.1.0/24, ...)
在专用网之间的隧道建立响应
(L2TP, 10.0.0.0/16, 10.1.0.0/16, 10.2.0.0/16, 10.0.0.0/24, 10.2.0.0/24, ...)
在专用网之间的ACK
(L2TP, 10.0.0.0/24, 10.2.0.0./24, 10.0.0.0/16, 10.1.0.0/16, ...)
VPN服务器设置
准备在专用网之间的隧道建立
(L2TP, 10.0.0.0/16, 10.1.0.0/16, 10.0.0.0/24, 10.2.0.0/24)
设置VPN客户机并驱动
建立VPN隧道
NAT设置
NAT设置
132
专用网连接管理表
网关B,
L2TP, 隧道ID
专用网A10.0.0.0/24
专用网B10.0.0.0/16
在隧道中的专用网A
的地址10.2.0.0/24
在隧道中的专用网B
的地址10.1.0.0/16
네트워크 인터페이스,
.....
132'
专用网连接管理表
网关A,
L2TP, 隧道ID
专用网B10.0.0.0/16
专用网A10.0.0.0/24
在隧道中的专用网B
的地址10.1.0.0/16
在隧道中的专用网A
的地址10.2.0.0/24
网络接口
.....

图 13